神州数码网络产品使用手册



DCRS-5526S(V3)
可堆叠千兆路由交换机

Version 1.1

http://www.dcnetworks.com.cn

前　言

DCRS-5526S 可堆叠千兆路由交换机，可作为大型企业网，校园网和城域网的汇聚设备，也可以适合中等规模办公环境的网络需求。DCRS-5526S 提供 24＋2 个端口，其中 24 个为固定配置的 10/100Base-TX 以太网接口，2 个为可选模块 M1、M2。M1 和 M2 可以插入的端口类型有 1000Base-TX 以太网接口、1000Base GBIC 接口、100Base-FX 单模/多模接口、100Base-T 以太网接口和 USB 堆叠接口。

为了使您能更好的了解、使用及日常维护 DCRS-5526S 交换机产品，我们特编写了本使用手册，希望您能在使用和配置交换机前仔细阅读一下本使用手册，以免损坏交换机或影响正常使用。在此，感谢您选择和购买了神州数码网络（北京）有限公司出品的系列网络产品，希望我们的产品和服务能让您满意，让“中国网络普遍成功”！

如果上述产品有软、硬件升级和变更，导致本使用手册内容需进行相应更新，恕不能事先通知。如需查询产品信息、更新产品软件和使用手册，请访问 http://www.dcnetworks.com.cn 的相应产品目录或咨询 800-810-9119 客户服务热线。

目 录

第1章 产品介绍

1.1 产品简介

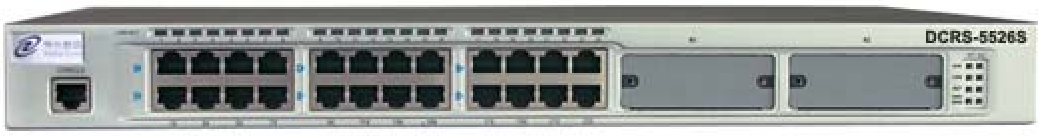


图 1-1 DCRS-5526S 交换机

1.1.1概述

DCRS-5526S 交换机可作为大型企业网、校园网和城域网的接入设备，也可以适合中等规模办公环境的网络需求。它具有独特的网络接入功能和灵活的网络控制功能，包括 MAC 绑定/过滤、MAC 地址数量限制、IEEE802.1Q VLAN、GVRP 动态注册 VLAN、PVLAN、IEEE802.1x 接入认证、QoS、ACL、带宽控制、IEEE802.3ad 端口汇聚、IGMP Snooping、广播风暴抑制、IEEE802.1D/w/s 生成树、端口镜像等。

1.1.2产品特点

■ 端口配置

DCRS-5526S 交换机提供了 24＋2 个端口，其中 24 个为固定配置的 10/100Base-TX 以太网接口， 2 个可选模块 M1 和 M2。M1 和 M2 可以插入的端口类型有 1000Base-TX 以太网接口、1000Base-X SFP 接口、1000M Combo 接口和专用堆叠接口、10/100Base-TX 以太网接口、100Base-X SFP 接口。

■ 堆叠方式

DCRS-5526S 交换机支持标准堆叠、经济堆叠和超级堆叠。通过超级堆叠，用户可以避开堆叠线缆的限制，使物理上相连的设备成为一个完整的堆叠组。DCRS-5526S 可以与 DCS-3900S 系列多种交换机进行混合堆叠，最多支持 9 台堆叠。

■ MAC 地址控制

DCRS-5526S 交换机除了支持标准的 MAC 地址动态学习功能以外，还扩展了多种基于 MAC 地址表的管理控制方式。MAC 地址绑定功能可以限制端口上连接设备的 MAC 地址，从而达到安全接入的目的。MAC 地址过滤功能可以按照源 MAC 地址进行过滤，以屏蔽一些非法接入设备。

■ VLAN 配置

DCRS-5526S 交换机支持标准的 IEEE802.1Q VLAN、端口保护 VLAN、PVLAN 和 GVRP 动态注册 VLAN。IEEE802.1 Q VLAN 可以将端口划分成多个 VLAN 组，最多可划分

4094 个，并且通过使用 IEEE802.1 Q VLAN
标记可以实现跨交换机的 VLAN 划分，同时达到控制了广播流量、保证安全性和网络性能的目的。PVLAN 功能可以将端口划分成隔离端口和团体端口，可按照网络应用需要隔离或连通端口。GVRP 动态注册 VLAN 可以基于 GARP 协议来实现网络内的 VLAN 动态注册，以减少由于 VLAN 配置变化而引起的更改 VLAN 配置的工作量，使 VLAN 应用更灵活。

■ **QoS**

DCRS-5526S 交换机支持丰富的 QoS 策略, 为每个端口提供了 4 个优先级队列，可分别设定队列带宽，支持 WRR/SP 调度方式。支持端口信任，可根据端口、VLAN、DSCP、IP 优先级、ACL 表进行流量分类，修改数据包的 DSCP 和 IP 优先级，并指定不同的带宽，为语音/数据/视频在同一网络中传输提供不同服务质量。

■ **ACL**

DCRS-5526S 交换机支持完整的 ACL 策略，ACL 是交换机实现的一种 IP 数据包过滤机制，通过允许或拒绝特定的数据包进出网络，交换机可以对网络访问进行控制，有效保证网络的安全运行。DCRS-5526S 交换机支持基于 IP、基于 MAC、基于 MAC-IP 的入口、出口过滤, 支持基于源/目的 IP 地址、源/目的 MAC 地址、IP 协议类型、TCP/UDP 端口号、IP Precendence、时间范围、ToS 等信息对数据进行过滤。

■ **IEEE8021.x 接入认证**

DCRS-5526S 交换机不但支持基于端口的 IEEE802.1x 认证模式，而且还支持基于 MAC 地址的 IEEE802.1x 认证模式，可以限制每个端口的最大接入认证用户数量，也可以基于 MAC 地址表实现动态的安全认证模式，还可以在正确认证后将此设备的 MAC 地址与端口绑定。通过这些 IEEE802.1x 认证方式与神州数码认证计费产品配合使用，可以提供一套完整的 IEEE802.1x 接入认证计费整体解决方案，满足接入、认证、计费的需求，保证网络安全性和可运营性。

■ **带宽控制（端口限速）**

DCRS-5526S 交换机支持上、下行带宽控制功能，可以为不同级别的用户分配不同的接入带宽，每个端口可以根据需要设置带宽速率，满足接入网对接入带宽控制的需要。

■ **端口汇聚**

DCRS-5526S 交换机支持 IEEE802.3ad 标准的端口汇聚，每个端口汇聚组由 2 至 8 个端口组成，并且可实现链路冗余和流量负载均衡。

■ **IGMP Snooping**

DCRS-5526S 交换机支持基于 IGMP Snooping 机制的组播应用，可以在接入网实现多种组播服务，降低网络流量，可满足多媒体播放、远程教学、娱乐等组播服务的需要。

■ **广播风暴抑制**

DCRS-5526S 交换机支持以数据包为单位的广播风暴抑制功能，可以有效的控制广播风暴，降低对带宽的无故占用，提升网络整体性能。

■ **生成树**

DCRS-5526S 交换机支持 IEEE802.1D 生成树、IEEE802.1w 快速生成树和 IEEE802.1s 多重生成树功能。生成树可以有效的避免环路的产生，同时实现链路的冗余备份。

■ **端口镜像**

DCRS-5526S 交换机支持端口镜像功能，此功能可以将某端口或某些端口的出入流量映射到另外一个端口来侦测相关的数据信息，可以用于排查网络故障和进行流量监测。

■ **DHCP 服务器、客户端**

DCRS-5526S 交换机支持 DHCP Server，可为设备动态分配主机 IP 地址，并可为指定 MAC 地址分配指定 IP 地址，从而实现 MAC 与 IP 绑定。

■ **RADIUS**

DCRS-5526S 交换机支持 RADIUS(远程拨号认证服务)认证协商。RADIUS 支持用户通过 IEEE802.1x 协议进行身份认证。

■ 全面的网络管理

DCRS-5526S 交换机可以通过 Console、Telnet、Web 和 SNMP 进行带外和带内管理。Console 和 Telnet 管理支持规范格式的 CLI（命令行界面），操作更简便、快捷，同时提供了中、英文双语提示。Web 管理提供了一个远程浏览式的图形化管理界面，使管理直观、便捷，快速查看工作状态，实时实现配置管理。SNMP 管理符合 V1、V2C 和 V3 标准版本，支持 Ether-Like MIB、Bridge MIB 和 MIB II，以及 RMON 1/2/3/9 MIB 等标准管理信息库，可以通过神州数码 LinkManager 中文网管软件系统实现完全的 SNMP 网络管理。DCRS-5526S 交换机支持 SSH 协议，可以最大限度地保证交换机的配置管理的安全性。DCRS-5526S 交换机还提供了独特的管理工作站 IP 设定功能，使得交换机可以自动过滤非法的远程网络管理连接，保证远程网络管理的有效性、安全性和一致性。

1.1.3主要特性

- 24 个 10/100Mbps 自适应 RJ-45 端口，所有端口均支持全双工/半双工工作模式
- 提供 2 个千兆扩展插槽，可选插 6 种扩展模块
- 其中 24 个为固定配置的 10/100Base-TX 以太网接口， 2 个可选模块 M1 和 M2。M1 和 M2 可以插入的端口类型有 1000Base-TX 以太网接口、1000Base SFP 接口、1000M Combo 接口和专用堆叠接口、10/100Base-TX 以太网接口、100M SFP 接口。

  ✧ **MS-GE-1SFP-B**
  MS-GE-1SFP-B 是具有 1 个 1000BASE-X SFP 端口的扩展模块
  ✧ **MS-SK-B**
  MS-SK-B 是具有 1 个专用堆叠接口的扩展模块
  ✧ **MS-GE-1GT-B**
  MS-GE-1GT-B 是具有 1 个 1000Base-TX 以太网接口的扩展模块
  ✧ **MS-GE-1GC-B**
  MS-GE-1GC-B 是具有 1 个 1000M Combo 接口的扩展模块
  ✧ **MS-FE-1TX-B**
  MS-FE-1TX-B 是具有 1 个 10/100Base-TX 以太网接口的扩展模块
  ✧ **MS-FE-1SFP-B**
  MS-FE-1SFP-B 是具有 1 个 100M SFP 接口的扩展模块

- 存储转发的交换方式，确保无阻塞传输
- 所有 RJ-45 端口均支持 MDI/MDI-X 自适应，可方便地使用直通双绞线级联到其它交换机上
- 支持全双工模式下的 IEEE802.3x 流量控制，半双工模式下的背压流量控制
- 提供 Console 控制端口
- 可查看端口的工作状态和统计数据
- 可进行本地和远程重新启动，以及恢复出厂设置
- 可通过 TFTP /FTP 进行固件升级

- 可安装在 19 英寸标准机架内

1.2 技术指标

- 协议与标准
  - IEEE802.3 10BASE-T 以太网
  - IEEE802.3u 100BASE-TX/FX 快速以太网
  - IEEE802.3x 流量控制
  - IEEE802.1x 网络访问控制
  - IEEE802.1D/w/s 生成树
  - IEEE802.1p 优先级控制
  - IEEE802.1Q VLAN
  - IEEE802.3ad 端口汇聚
  - TFTP/FTP
  - DHCP
  - BootP
  - Telnet
  - IP/UDP/TCP/ICMP
  - HTTP
  - SNMP V1/V2C/V3
- 管理标准及方式
  - CLI 命令行
  - 支持 SNMP V1/V2C，可通过 LinkManager 中文网管软件系统进行管理
  - 支持 Web 和 Telnet 管理
  - RFC1757 RMON（1、2、3、9）
- MIB 库
  - RFC1213 MIB II
  - RFC1493 Bridge MIB
  - RFC1643 Ether-Like MIB
  - DigitalChina Private MIB

1.3 物理特性

- 控制口
  - 1 个 RJ-45 型串口
- 交流电源输入
  - 100～240VAC，50～60Hz
  - 内置通用电源
- 电源功耗
  - 最大 50W
- 运行温度
  - 0°C～50°C

- 储藏温度
  - -40°C～70°C
- 相对湿度
  - 5%～95%，无凝结
- 尺寸
  - DCRS-5526S ：440mm×236mm×44mm
- 重量
  - DCRS-5526S ：3kg
- 平均无故障时间
  - 最低 80，000 小时 MTBF

1.4 产品外观

1.4.1产品前面板

DCRS-5526S 交换机的前面板上有 24 个 10/100Mbps 自适应 RJ-45 端口、2 个扩展插槽、1 个 Console 端口和 32 个 LED 指示灯。DCRS-5526S 交换机前面板如下图所示：

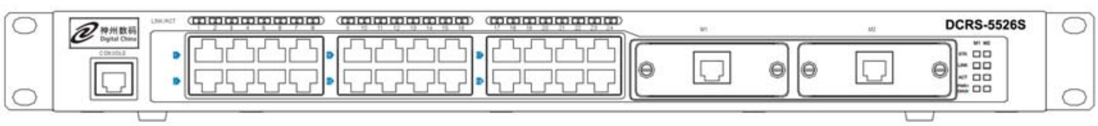


图 1-2 DCRS-5526S 交换机前面板

1.4.2产品后面板

DCRS-5526S 交换机的后面板上有 1 个电源插槽（100～240VAC，50～60Hz）。DCRS-5526S 交换机后面板如下图所示：



图 1-3 DCRS-5526S 交换机后面板

1.4.3LED 指示灯

DCRS-5526S 交换机的 LED 指示灯包括：Stack、Link/Act、Power 和 Diag.指示灯，如下图所示：

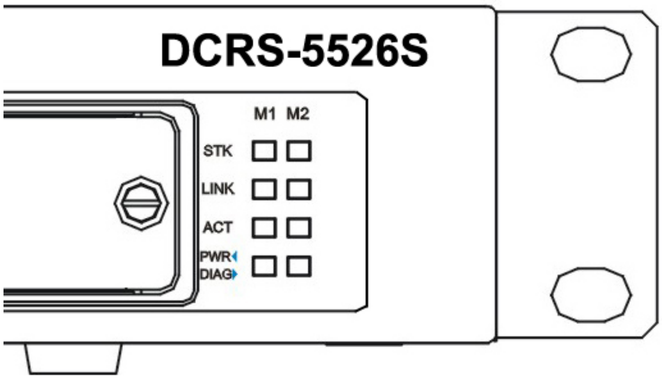


图 1-4 DCRS-5526S 交换机 LED 指示灯

LED 指示灯状态描述：

LED	状态		说明
1-24X（右）	点亮		端口 link 成功。
	熄灭		端口 link 失败或未连接。
1-24X（左）	闪烁		端口 link 成功，正在收发数据。
	熄灭		端口无数据收发。
Stack(1/2)	点亮		扩展 USB 堆叠模块连接。
	熄灭		扩展 USB 堆叠模块未连接。
Link(1/2)	点亮		千兆模块 link 成功。
	熄灭		千兆模块 link 失败或未连接。
ACT(1/2)	闪烁		千兆模块正在收发数据。
	熄灭		千兆模块无数据收发。
Power	点亮		电源已接通。
	熄灭		电源未接通。
Diag(诊断、堆叠复用)	诊断	闪烁	程序初始化。
		点亮	程序初始化结束。
		熄灭	程序初始化失败。
	堆叠	点亮	本机为堆叠组中的 Master。
		熄灭	本机为堆叠组中的 Slave。

表 1-1 DCRS-5526S 交换机 LED 指示灯描述

第2章 硬件安装

2.1 安装须知

在 DCRS-5526S 交换机的安装和使用中，为了您和他人的人身安全，以及确保正常使用交换机，请仔细阅读如下安装注意事项和提示。

2.1.1安装环境要求

- 交换机必须工作在清洁的环境中，应保持无灰尘堆积，以避免静电吸附而导致器件损坏。
- 交换机必须工作在室内环境温度 0～50°C、湿度 5～95%无凝结的环境中。
- 交换机必须置于干燥阴凉处，四周都应留有足够的散热间隙，以便通风散热。
- 交换机必须工作在 100 ~ 240VAC（50 ~ 60Hz）的供电范围内。
- 交换机必须有效接地，以避免静电损坏交换机和漏电造成人身伤害。
- 交换机必须避免阳光直射，远离热源和强电磁干扰源。
- 交换机必需可靠的、稳固的安装到桌面上或标准 19 英寸机架上。

2.1.1.1安装环境清洁度

灰尘对交换机运行安全是一种危害。室内灰尘可以造成静电吸附，使金属接件或金属接点接触不良。尤其是在室内相对湿度偏低的情况下，更易造成这种静电吸附，不但会影响交换机的寿命，而且容易造成交换机故障。机房推荐的工作环境灰尘含量及粒径如下表所示：

最大直径（μm）	0.5	1	3	5
最大浓度 （每立方米所含颗粒数）	1.4×10^7	7×10^5	2.4×10^5	1.3×10^5

表 2-1　机房推荐的工作环境灰尘含量及粒径

除灰尘外，交换机对空气中所含的盐、酸、硫化物也有严格的要求。这些有害气体会加速金属的腐蚀和某些部件的老化。机房内应防止有害气体如 SO_2、H_2S、NO_2、NH_3、CL_2 等的侵入，机房推荐的工作环境有害气体限制值如下表所示：

气体	平均（mg/m^3）	最大（mg/ m^3）
二氧化硫 SO_2	0.2	1.5
硫化氢 H_2S	0.006	0.03
二氧化氮 NO_2	0.04	0.15
氨 NH_3	0.05	0.15
氯气 Cl_2	0.01	0.3

表 2-2　机房推荐的工作环境有害气体限制值

2.1.1.2温湿度

由于交换机采用低噪音设计。在安装完交换机后要注意空气的对流通风，建议安装在能维持一定温度和湿度的室内机房中的机架上。如果夏天气温较高，建议使用空调等降温设备；如果冬季气温较低，建议加装暖气等增温设备。若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件腐蚀等现象；若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，同时在干燥的气候环境下，易产生静电，危害交换机的电路；温度过高会使交换机的可靠性降低，长期高温还会影响其使用寿命，过高的温度将加速绝缘材料的老化过程。机房推荐的工作温湿度如下表所示：

温度		相对湿度	
长期工作条件	短期工作条件	长期工作条件	短期工作条件
15～30℃	0～50℃	40～65%	10～95%

表 2-3　机房推荐的工作环境温湿表

注意：

交换机机房内工作环境温、湿度的测量点是指在机架前后没有保护板时测量，距地面 1.5m 和距机架前面 0.4m 处测量的数值。短期工作条件是指连续工作不超过 48 小时和每年累计不超过 15 天。极端恶劣工作条件是指机房空调系统出现故障时可能出现的环境温度和相对湿度，每次不应超过 5 小时就应恢复正常工作范围。

2.1.1.3电源

交换机采用模块开关电源，对交流电源输入参数如下：

输入电压：100-240VAC

频率：50-60Hz

整机功耗：≤50W

接通电源前建议先检查电源输入，确保供电系统接地良好和交换机输入端电源稳定可靠，必要时可安装电压调节装置。电路短路保护措施中应保证有一个不大于 240V、10A 的保险丝或断路器在相线中。为保证提供稳定、可靠的电源，建议使用 UPS 不间断电源。

警告：

若供电系统没有良好接地，输入电源抖动过大或存在过度脉冲，都会引起交换机误码率增加，甚至损坏硬件器件！

2.1.1.4防静电

静电会对交换机的电路和整机产生破坏作用。为防止静电的危害，应做到交换机及地板良好、有效接地，机房室内防尘及除尘，保持适当的温湿度，操作人员穿着防静电服装和佩戴防静电手环、手套。

2.1.1.5抗干扰

各种干扰源，无论是来自交换机或其它设备，无论来自内部还是来自外部，都是以电容耦合、电感耦合、电磁波辐射、公共阻抗（包括接地系统）和导线（电源线、信号线和输出线等）的传导方式对交换机产生影响。因此要注意如下事项：

- 要对供电系统采取有效的防电网干扰措施。
- 交换机工作接地最好不要和电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些。
- 远离强功率无线电发射台、雷达发射台和高频大电流设备。
- 必要时采取电磁屏蔽的方法。

2.1.1.6机架配置

交换机的尺寸是按照 19 英寸标准机柜设计的，交换机整体尺寸大小为长×宽×高=440mm×236mm×44mm。至于通风散热，请注意如下情况：

- 机架上每一台设备工作时都会发热，因此封闭的机架必须有散热口和冷却风扇，而且设备不能放得太密集，以确保通风散热良好。
- 在开放的机架上安装交换机时，注意机架的框架不要挡住交换机两侧的通风孔。在安装好交换机后要仔细检查交换机的安装状态，防止上述情况发生。

⚠ **注意：**

如果没有 19 英寸标准机柜，那么就需要将交换机安装在平稳的、干净的桌面上，同时四周要留出 10mm 的散热空间，同时不要在交换机上面放置重物。

2.1.2安装操作提示

- 在安装开始前，先仔细阅读本使用手册中的相关章节或参加相关技术培训；然后，准备好安装所需的材料、工具和相关用品；同时，准备好适合的安装场地，以便安装调试。
- 在安装过程中，必须使用包装箱内附带的专用机架安装角铁和螺丝钉；必须使用合适的安装工具，保证安装稳固、可靠；必须穿着合身的防静电服装和佩戴防静电手环、手套，以免损坏交换机；必须使用合格的、规格正确线缆和接头，并按标准制作线缆；必须注意安装环境存在的潜在危险，做好防护措施，避免意外伤害。
- 在安装完成后，注意清理安装现场，保持干净、整洁；注意在交换机通电前将交换机进行有效的接地；要定期对所安装的交换机进行维护，以延长交换机的使用寿命。

2.1.3安全警告

- 不要尝试可能引起人身伤害、意外事故或损坏交换机的安装操作。
- 不要在带电状态下安装、移动和拆卸交换机及模块，以避免造成人身伤害和设备损坏。
- 不要私自拆开交换机，有故障可直接送修，以避免造成人身伤害和设备损坏。
- 不要将金属物接触带电电源或掉入交换机内部，以避免短路和器件损坏。

- 不要在带电状态下触摸电源插头和插座，
  以免触电造成人身伤害。
- 不要将易燃物堆放在交换机周围，以免发生火灾。
- 不要在有潜在危险的情况下单独安装调试交换机，以应付突发意外事故。
- 要使用标准的、有过载和漏电保护的电源插座，以免发生意外事故。
- 要经常检查和维护电路和安装、工作环境是否存在安全隐患，做好预防工作。
- 要将紧急电源开关安装在工作间中，以便在意外事故发生可以迅速切断电源。

⚠ **注意:**

可能的潜在危险和安全隐患包括：电源漏电、电源打火、电线破损、接地不良、电路过载和电路短路等。如果遇到触电、火灾、短路等意外情况发生，请迅速切断电源，并立即报警。在不危急自身安全的前提下，救助在意外事故中的伤者，并根据受伤害情况对伤者采取适当的急救措施，并可通过各种方式向专业医疗急救机构寻求帮助。没有医疗救助经验者，切勿随意、胡乱处置伤者，待专业医疗急救人员到场后再进行相应的处置。

2.2 安装准备

2.2.1核对装箱单

首先打开交换机的包装箱，仔细核对包装箱内的交换机及附件是否齐全。如果发现包装箱内有任何物品的缺失或损坏，请立即与销售该产品的经销商或者与当地神州数码网络公司的相关人员联系。

对于一台标准配置的 DCRS-5526S 交换机，包装箱内应包含如下物品：

序号	名称	数量
1	DCRS-5526S 以太网交换机	1 台
2	AC 电源线	1 根
3	使用光盘	1 张
4	Console 线缆	1 根
5	Console 转接头	1 个
6	机架角铁	2 个
7	机架安装螺钉	4 个
8	保修卡	1 张
9	合格证	1 张

表 2-4　DCRS-5526S 系列交换机装箱单

注：上述内容以实际产品所附带的装箱单为准。

2.2.2安装工具及材料

需要工具和服装	● 十字改锥
	● 一字改锥
	● 打线钳
	● 防静电服装
	● 防静电手环
	● 防静电手套
连接电缆	● Console 线缆和转接头
	● 标准双绞线
	● RJ-45 插头

表 2-5　安装工具及材料表

2.3 硬件安装

2.3.1在机架上安装交换机

DCRS-5526S 交换机可以安装于标准的 19 英寸机架内。请按照如下步骤安装交换机：

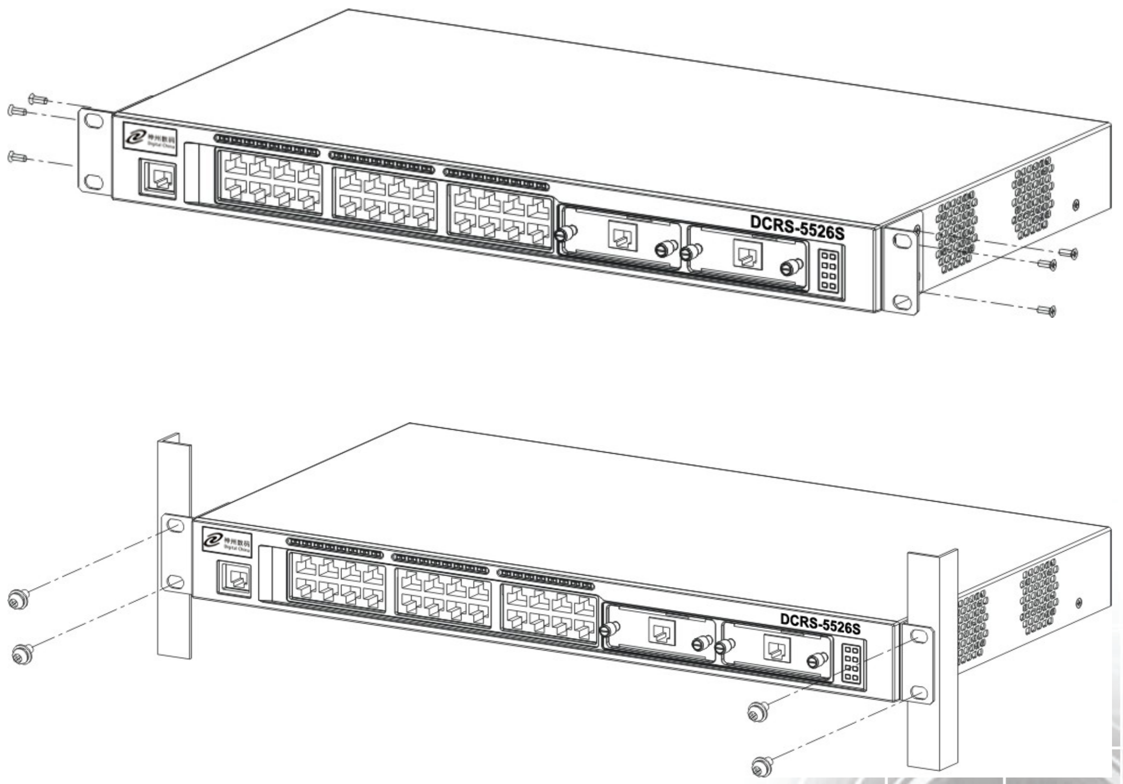


图 2-1　DCRS-5526S 系列交换机在机架上安装

1. 用包装箱内附带的机架安装螺丝钉将专用机架角铁牢固的安装到交换机的两侧。

2. 将交换机置于标准 19 英寸机架内，
   再使用螺丝钉将交换机牢固的固定在机架中的合适位置，并且在交换机与周围物体间留有足够的通风空间。

注意：

交换机的角铁起的是固定作用，不能用来承重，建议在交换机底部安装机架托板，并且不要在交换机上放置重物，也不要让其它设备或物体遮挡住交换机的通风孔，以免损坏交换机或影响交换机正常工作。

2.3.2在交换机上安装模块

DCRS-5526S 交换机可以选插 6 种模块，可以通过这些模块实现与网络骨干或其它交换机的连接。请按照如下步骤安装模块：

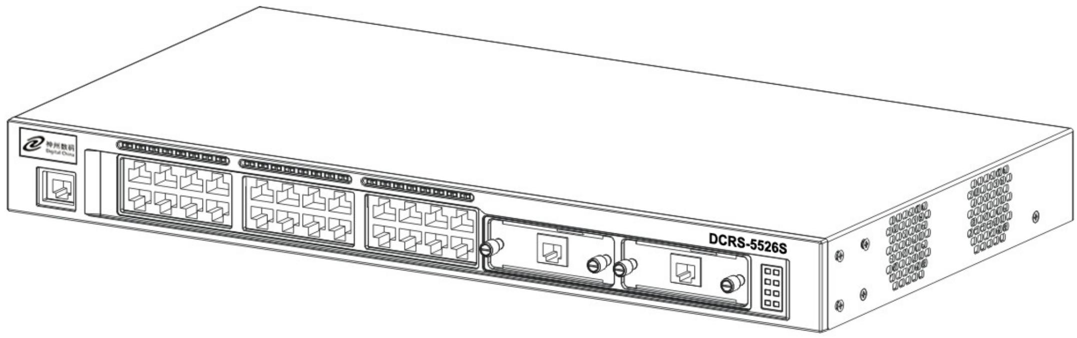


图 2-2　在 DCRS-5526S 系列交换机上安装模块

3. 切断交换机电源，卸下对应扩展模块插槽的空白挡板，并将卸下的挡板保存好以便日后使用。
4. 在打开模块包装前，确保已通过接地除去身上的静电，有条件的化可以穿着防静电服装和佩戴防静电手环、手套，以免静电损坏模块。
5. 从防静电袋中取出模块，沿对应扩展模块插槽中的导轨水平插入模块（箭头方向），直到模块与扩展模块插槽内的接插件紧密连接。
6. 拧紧模块挡片上的螺丝钉，使模块牢固的安装在扩展模块插槽中。

注意：

由于模块不支持热插拔，不可以带电插拔模块，所以在安装前必须切断交换机电源，不

然可能会损坏交换机或模块。由于模块的电路
板是裸露的，所以在安装模块时要特别注意防静电，应采取相应的防静电措施（接地放静电、穿着防静电服装、佩戴防静电手环、手套），以免损坏交换机和模块。

2.3.3Console 线缆连接

DCRS-5526S 交换机提供了一个 RJ-45 型的异步串行 Console 配置口。请按照如下步骤连接 Console 线缆：

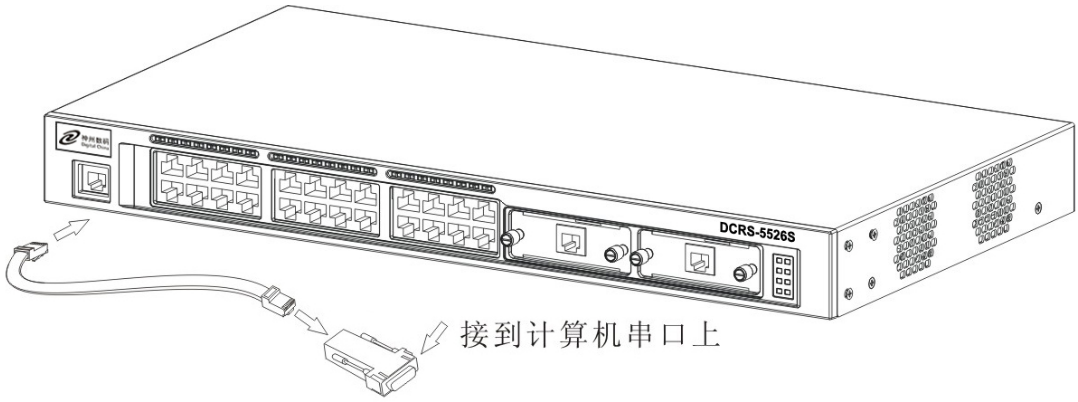


图 2-3 将 Console 线缆连接到 DCRS-5526S 系列交换机上

1. 将包装箱中附带的 Console 线缆一端的 RJ-45 接头连接到交换机的 Console 端口中。
2. 将 Console 另一端连接到一台字符终端（通常是计算机）上。
3. 在交换机和字符终端都已加电后，通过字符终端可以与交换机建立管理配置连接。

注意：

请使用交换机附带的 Console 线缆和 Console 转接头，不要将 Console 线缆误插到其它端口中，也不要将其它线缆误插到 Console 端口中，以免损坏线缆和端口。

2.3.4电源线连接

DCRS-5526S 交换机的电源规格是 100～240VAC，50～60Hz，可以适应一定范围内的电压浮动。请按照如下步骤连接电源线：

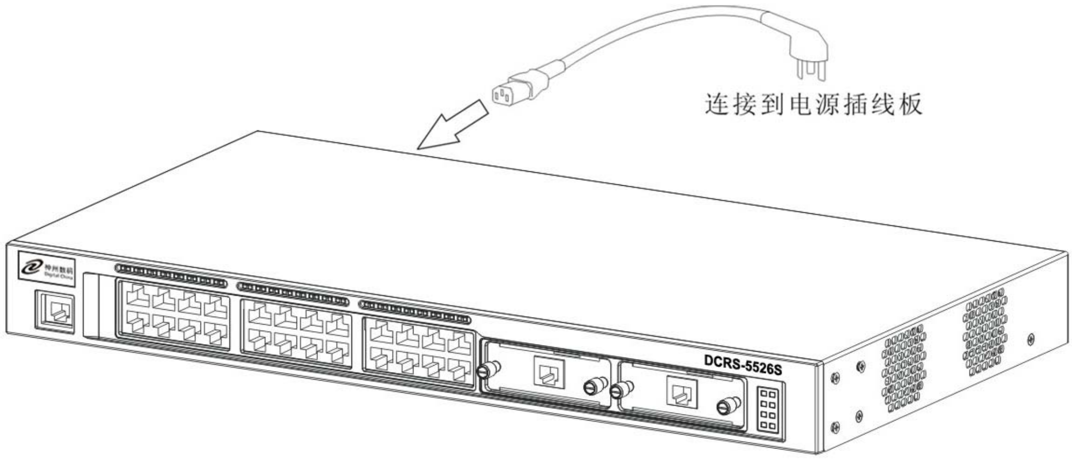


图 2-4　将电源线连接到 DCRS-5526S 系列交换机上

1. 将包装中附带电源线的一端插到交换机后面板上的电源插槽中，另一端插到标准的带过载和漏电保护的电源插座上。
2. 检查交换机前面板上的 Power 指示灯是否已亮。DCRS-5526S 交换机可根据电源的输入电压自动调节。因此，只要输入电压符合后面板上所标明的电压范围，交换机就可正常运行，而无需额外的调试。
3. 交换机加电后，将自动执行自检。

注意:

输入电压必须符合交换机电源规格，不然可能损坏交换机或使交换机工作不正常，减少使用寿命。如果电源加电后 Power 指示灯不亮或自检不正常，请与经销商或神州数码网络客服中心联系，不要擅自拆卸交换机机壳，以免造成损失和人身伤害。

第3章 Setup 配置

我们所说的 Setup 配置，是指用户购买交换机设备以后，第一次对交换机进行的操作。对首次使用 DCRS-5526S 交换机的用户，Setup 配置具有很强的指导性。当然，用户使用 CLI 配置界面时，在特权用户模式下输入命令 **setup**，也可以进入到 Setup 配置界面。

3.1 Setup 配置

Setup 是以菜单的形式进行配置的，在 Setup 配置模式中可以对交换机的主机名、Vlan1 接口、Telnet 服务、Web 服务、SNMP 等进行配置。

3.2 Setup 主菜单

在进入主菜单之前，会提示用户选择配置界面的语言种类。对英文不是很熟悉的用户可以选择“1”，进入中文提示的配置界面；如果选择“0”，则进入英文提示的配置界面。

Please select language:

[0]:English

[1]:中文

Selection(0|1)[0]:

下面是 Setup 的英文主菜单的提示：

Configure menu

[0]:Config hostname

[1]:Config interface-Vlan1

[2]:Config telenet-server

[3]:Config web-server

[4]:Config SNMP

[5]:Exit setup configuration without saving

[6]:Exit setup configuration after saving

Selection number:

其对应的中文主菜单的提示为：

配置菜单

[0]:配置交换机主机名

[1]:配置 Vlan1 的接口

[2]:配置交换机 Telnet 服务器

[3]:配置交换机 Web 服务器

[4]:配置 SNMP

[5]:退出 setup 模式不保存配置结果

[6]:退出 setup 模式保存配置结果

选择序号:

3.3 Setup 子菜单

3.3.1配置交换机的主机名

在 Setup 主菜单上选择“0”，回车出现如下提示：

Please input the host name[DCRS-5526S]:

其对应的中文提示为：

请输入交换机主机名[DCRS-5526S]:

注意：用户输入的主机名长度应当小于 30 个字符。如果用户没有输入任何值而直接按回车键，则主机名为缺省的“DCRS-5526S”。

3.3.2配置 Vlan1 的接口

在 Setup 主菜单上选择“1”，回车出现如下提示，开始对 Vlan1 的接口进行配置：

Config Interface-Vlan1

[0]: Config interface-Vlan1 IP address

[1]: Config interface-Vlan1 status

[2]: Exit

Selection number:

其对应的中文提示为：

配置 Vlan1 接口

[0]: 配置 Vlan1 接口的 IP 地址

[1]: 配置 Vlan1 接口的状态

[2]: 返回上一级菜单

选择序号:

如果在 Vlan1 的接口配置菜单中选择“0”，回车出现如下提示：

Please input interface-Vlan1 IP address (A.B.C.D):

其对应的中文提示为：

请输入 Vlan1 接口的 IP 地址(A.B.C.D):

在用户输入 Vlan1 接口有效的 IP 地址后，回车出现如下提示：

Please input interface-Vlan1 mask [255.255.255.0]:

其对应的中文提示为：

请输入 Vlan1 接口的子网掩码 [255.255.255.0]:

系统缺省设置 Vlan1 接口的掩码为 255.255.255.0。用户可以根据实际网络环境配置 IP 地址及掩码，配置完毕后，返回到 Vlan1 的接口配置菜单。

如果在 Vlan1 的接口配置菜单中选择“1”，回车出现如下提示：

Open interface-Vlan1 for remote configuration ? (y/n) [y]:

其对应的中文提示为：

是否打开 Vlan1 的接口? (y/n) [y]:

在首次开机时，系统的 Vlan1 接口（即 CPU 端口）是处于关闭状态的，需要通过本命令打开交换机的 Vlan1 接口。直接回车表示打开交换机的 Vlan1 接口。

如果在 Vlan1 的接口配置菜单中选择“2”，则返回到 Setup 主菜单。

3.3.3配置 Telnet 服务器

在 Setup 主菜单上选择“2”，回车出现如下提示，开始对 Telnet 服务器进行配置：

Configure telnet server

[0]: Add telnet user

[1]: Config telnet server status

[2]: Exit

Selection number:

其对应的中文提示为：

配置 Telnet 服务器

[0]: 添加 Telnet 服务器用户

[1]: 配置 Telnet 服务器的状态

[2]: 返回上一级菜单

选择序号:

如果在 Telnet 服务器配置菜单中选择“0”，回车出现如下提示：

Please input the new telnet user name :

其对应的中文提示为：

请输入要添加的 Telnet 用户名:

注意：用户名的有效长度为 1~16 个字符。在用户输入有效的用户名后，回车出现如下提示：

Please input the new telnet user password :

其对应的中文提示为：

请输入用户密码:

注意：密码的有效长度为 1~8 个字符。在用户配置完用户名和密码后，返回到 Telnet 服务器配置菜单。

如果在 Telnet 服务器配置菜单中选择“1”，回车出现如下提示：

Enable switch telnet-server or no?(y/n) [y]:

其对应的中文提示为：

是否使能交换机 Telnet 服务器?(y/n) [y]:

如果用户需要启动 Telenet 服务，则输入“y”回车或直接回车；如果用户不需要启动 Telenet 服务，则输入“n”回车。然后返回到 Telnet 服务器配置菜单。

如果在 Telnet 服务器配置菜单中选择“2”，
则返回到 Setup 主菜单。

3.3.4配置 Web 服务器

在 Setup 主菜单上选择“3”，回车出现如下提示，开始对 Web 服务器进行配置：

Configure web server

[0]: Add webuser

[1]: Config web server status

[2]: Exit

Selection number:

其对应的中文提示为：

配置 Web 服务器

[0]: 添加 Web 服务器用户

[1]: 配置 Web 服务器的状态

[2]: 返回上一级菜单

选择序号:

如果在 Web 服务器配置菜单中选择“0”，回车出现如下提示：

Please input the new web user name :

其对应的中文提示为：

请输入要添加的 Web 用户名:

注意：用户名的有效长度为 1~16 个字符。在用户输入有效的用户名后，回车出现如下提示：

Please input the new web user password :

其对应的中文提示为：

请输入用户密码:

注意：密码的有效长度为 1~8 个字符。在用户配置完用户名和密码后，返回到 Web 服务器配置菜单。

如果在 Web 服务器配置菜单中选择“1”，回车出现如下提示：

Enable switch web-server or no?(y/n) [y]:

其对应的中文提示为：

是否使能交换机 Web 服务器?(y/n) [y]:

如果用户需要启动 Web 服务，则输入“y”回车或直接回车；如果用户不需要启动 Web 服务，则输入“n”回车。然后返回到 Web 服务器配置菜单。

如果在 Web 服务器配置菜单中选择“2”，则返回到 Setup 主菜单。

3.3.5配置 SNMP

在 Setup 主菜单上选择“4”，回车出现如下提示，开始对 SNMP 进行配置：

Configure SNMP

[0]: Config SNMP-server read-write community string

[1]: Config SNMP-server read-only community string

[2]: Config traps-host and community string

[3]: Config SNMP-server status

[4]: Config SNMP traps status

[5]: Add SNMP NMS security IP address

[6]: Exit

Selection number:

其对应的中文提示为：

配置 SNMP

[0]: 配置 SNMP 读写访问团体字符串

[1]: 配置 SNMP 只读访问团体字符串

[2]: 配置 Traps 主机 IP 地址和团体字符串

[3]: 配置交换机 SNMP 状态

[4]: 配置交换机 Traps 状态

[5]: 添加 SNMP 管理站安全 IP 地址

[6]: 返回上一级菜单

选择序号:

如果在 SNMP 配置菜单中选择"0"，回车出现如下提示：

Please input the read-write access community string[private]:

其对应的中文提示为：

请输入 SNMP 读写访问团体字符串[private]:

注意：读写访问团体字符串的有效长度为 1~255 个字符，缺省值为"private"。在用户输入有效的读写访问团体字符串后，回车返回到 SNMP 配置菜单。

如果在 SNMP 配置菜单中选择"1"，回车出现如下提示：

Please input the read-only access community string[public]:

其对应的中文提示为：

请输入 SNMP 只读访问团体字符串[public]:

注意：只读访问团体字符串的有效长度为 1~255 个字符，缺省值为"public"。在用户输入有效的只读访问团体字符串后，回车返回到 SNMP 配置菜单。

如果在 Vlan1 的接口配置菜单中选择"2"，回车出现如下提示：

Please input traps-host IP address(A.B.C.D):

其对应的中文提示为：

请输入接收 Traps 的主机 IP 地址(A.B.C.D):

在用户输入有效的接收 Traps 主机的 IP 地址后，回车出现如下提示：

Please input traps community string[public]:

其对应的中文提示为：

请输入通信团体字符串[public]:

注意：通信团体字符串的有效长度为 1~255 个字符，缺省值为"public"。在用户输入有效的通信团体字符串后，回车返回到 SNMP 配置菜单。

如果在 SNMP 配置菜单中选择"3"，回车出现如下提示：

Enable SNMP-server? (y/n) [y]:

其对应的中文提示为：

是否使能交换机 SNMP? (y/n) [y]:

如果用户需要启动 SNMP 服务，则输入"y"回车或直接回车；如果用户不需要启动 SNMP 服务，则输入"n"回车。然后返回到 SNMP 配置菜单。

如果在 SNMP 配置菜单中选择"4"，回车出现如下提示：

Enable SNMP-traps ? (y/n) [y]:

其对应的中文提示为：

是否使能交换机发送 Traps ? (y/n) [y]:

如果用户需要交换机能够发送消息给 Traps，则输入"y"回车或直接回车；如果用户不需要发送，则输入"n"回车。然后返回到 SNMP 配置菜单。

如果在 SNMP 配置菜单中选择"5"，回车出现如下提示：

Please input the new NMS IP address(A.B.C.D):

其对应的中文提示为：

请输入要添加的 SNMP 管理站安全 IP 地址(A.B.C.D):

在用户输入有效的 SNMP 管理站的安全 IP 地址后，回车返回到 SNMP 配置菜单。

如果在 SNMP 配置菜单中选择"6"，则返回到 Setup 主菜单。

3.3.6退出 Setup 配置模式

在 Setup 主菜单上选择"5"， 用户退出 Setup 配置模式，同时用户在 Setup 模式下所做的配置均不保留。

在 Setup 主菜单上选择"6"， 用户退出 Setup 配置模式，同时用户在 Setup 模式下所做的配置均保留。例如用户在 Setup 配置模式下，设置了 IP 地址、打开了 Web 服务，选择"6"退出 Setup 主菜单后，用户就可以利用终端，通过 Telnet 服务对交换机进行管理配置。

用户从 Setup 配置模式退出后，进入到 CLI 配置界面。有关 CLI 的配置命令及语法在以后的章节中有详细介绍。

第4章 交换机管理

4.1 管理方式

用户购买到交换机设备后，需要对交换机进行配置，从而实现对网络的管理。DCRS-5526S 为用户提供了两种管理方式：带外管理和带内管理。

4.1.1带外管理

带外管理（Out-band management）：即通过 Console 口对交换机进行配置管理。通常情况下，在首次配置交换机或者无法进行带内管理时，用户会使用带外管理方式。例如：用户希望通过远程 Telnet 或 HTTP 来访问交换机时，必须首先通过 Console 口给交换机配置一个 IP 地址。

用户进行带外管理的步骤如下。

第一、搭建环境：

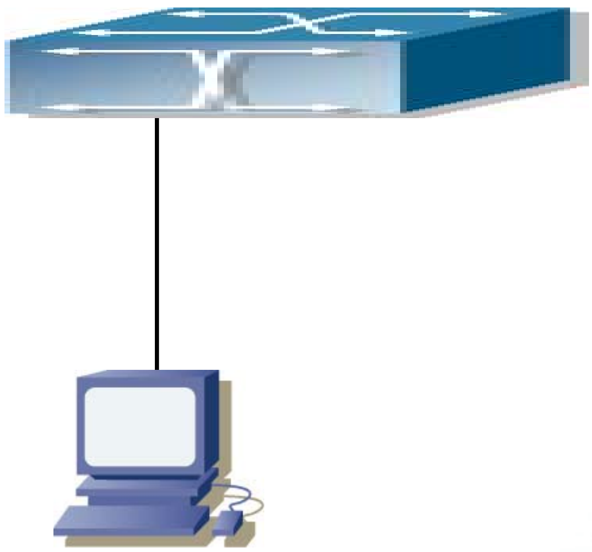


图 4-1　DCRS-5526S 带外管理配置环境

按照图所示将 PC 的串口（RS-232 接口）和交换机通过随机提供的串口线连接，下面是连接中用到的设备说明：

设备名称	说明
PC 机	有键盘、有完好的 RS-232 串口、并且安装终端仿真程序，如

	Windows 9x/NT/2000/XP 自带超级终端等。
串口线	一端与 PC 机的 RS-232 串口相连；另一端与 DCRS-5526S 的 Console 口相连。
DCRS-5526S	有完好的 Console 口。

第二、进入超级终端：

连接成功后，打开 Windows 系统自带超级终端。下面是打开 Windows XP 自带超级终端的示例。

1）点击超级终端：

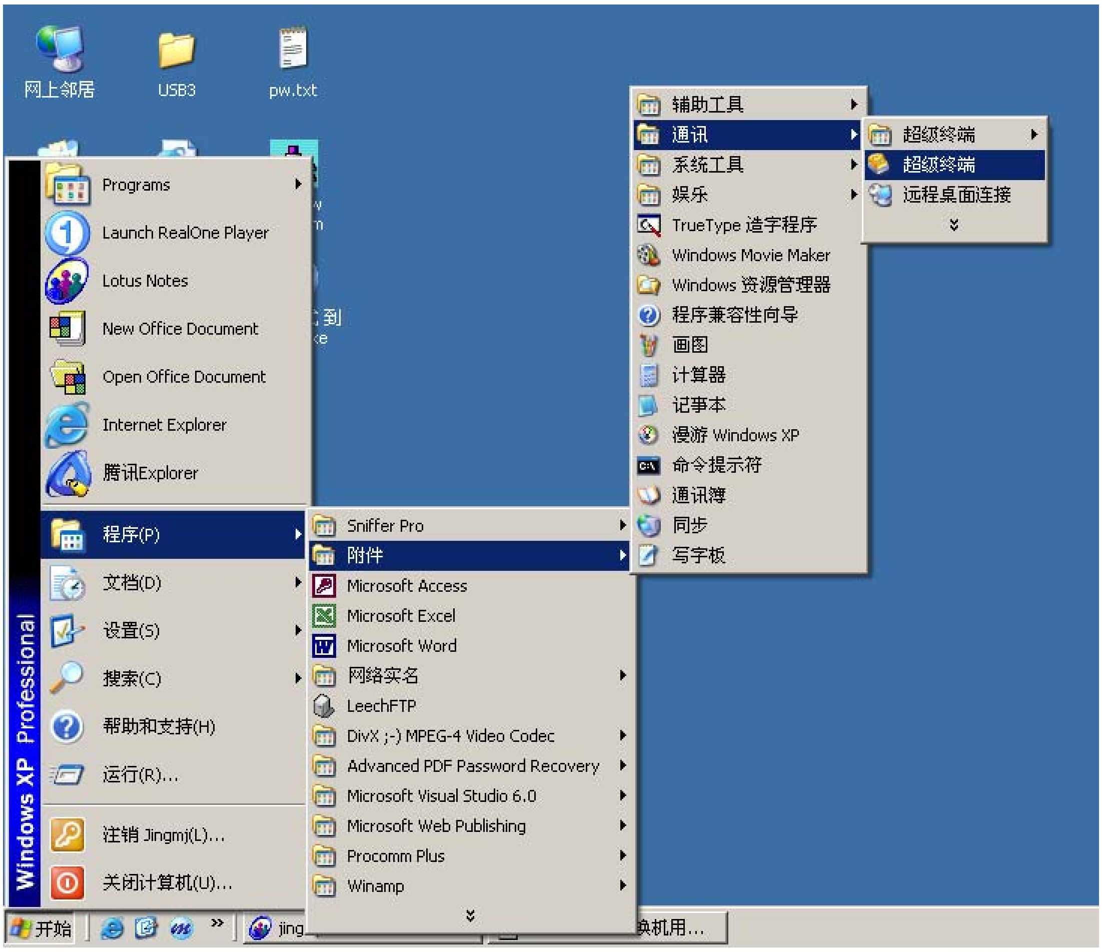


图 4-2 打开超级终端一

2）在“名称”处填入打开超级终端的名称，如把它定义为“DCRS5526”：



图 4-3 打开超级终端二

3）在"连接时使用"处，选择 PC 机使用的 RS-232 串口，如连接的是串口 1，则选择串口 1，点击确定按钮：

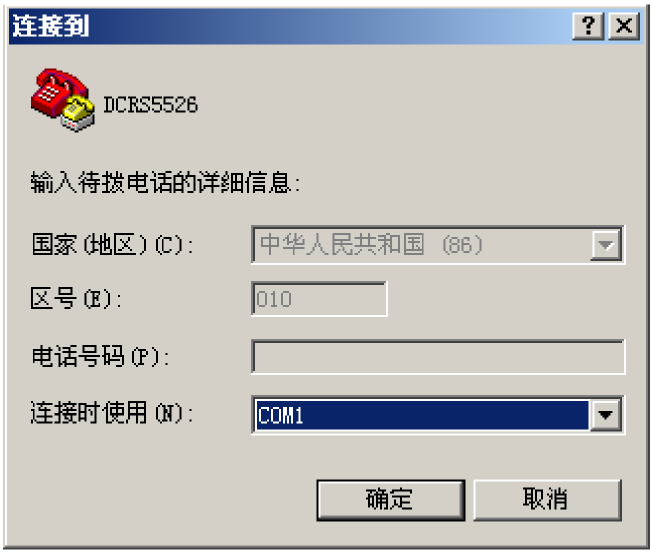


图 4-4 打开超级终端三

4）出现 COM1 属性，波特率选择"9600"，数据位选择"8"，奇偶校验选择"无"，停止位选择"1"，流量控制选择"无"；或者直接点击"还原默认值"后，流量控制项选择"无"，点击确定按钮：

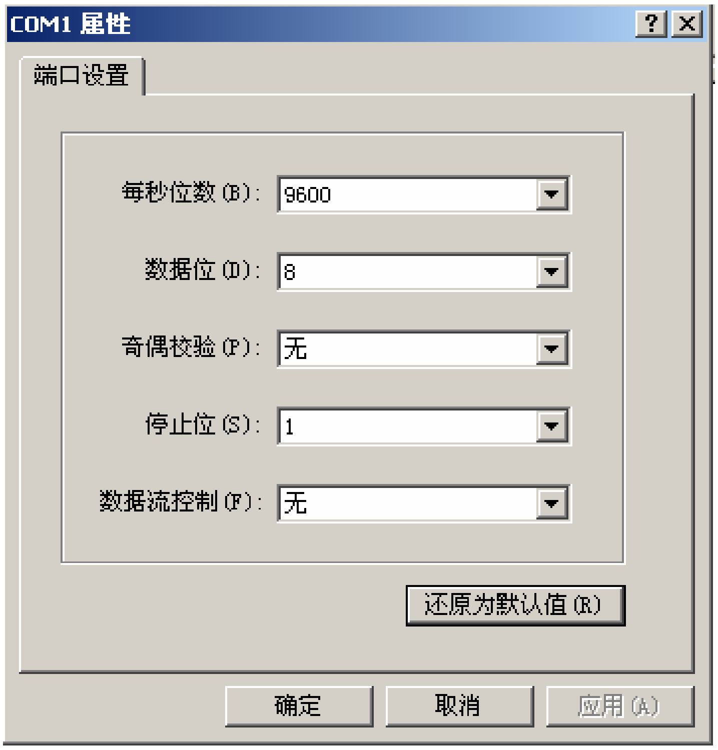


图 4-5 打开超级终端四

5）出现超级终端的配置界面：

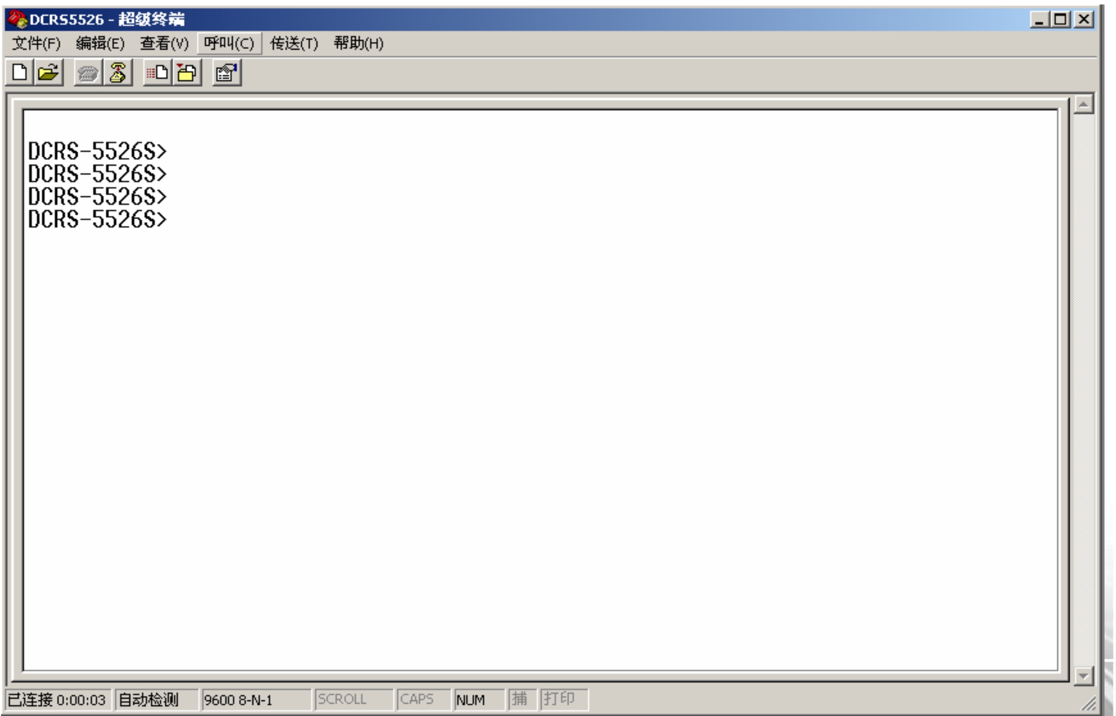


图 4-6 打开超级终端五

第三、进入交换机 CLI 界面：

打开交换机的电源开关。在超级终端的配置界面上出现了如下提示，进入到DCRS-5526S 的 CLI 配置方式：

DigitalChina Inc

Copyright (c) 2003 by DigitalChina Networks Ltd.

All rights reserved.

Testing RAM...

67,108,864 RAM OK.

Loading system...

Starting system...

Current time is MON JAN 01 00:00:00 2001

DCRS-5526S Series Switch Operating System, Version RW-0.0.42

Copyright (C) 2001-2002 Digital China Networks Limited

http://www.dcnetworks.com.cn

DCRS-5526S Switch (MPC8245-266M) processor

24 Ethernet/IEEE 802.3 interface(s)

DCRS-5526S>

接下来用户可以输入相关命令进行管理，各命令详见后面章节的相关内容。

4.1.2带内管理

所谓带内管理（In-band management），即通过 Telnet 程序登录到交换机，或者通过 HTTP 协议访问交换机，或者通过神州数码网络（北京）有限公司自主研发的网管软件 LinkManager 对交换机进行配置管理。交换机提供带内管理方式可以使连接在交换机中的某些设备具备管理交换机的功能。当交换机的配置出现变更，导致带内管理失效时，可以使用

带外管理对交换机进行配置管理。

4.1.2.1通过 Telnet 管理交换机

通过 Telnet 管理交换机要具备的条件：

1) 交换机配置 IP 地址；
2) 作为 Telnet 客户端的主机 IP 地址与其所属交换机的 VLAN 接口的 IP 地址在相同网段；
3) 若不满足 2)，则 Telnet 客户端可以通过路由器等设备到达交换机某个 IP 地址。

DCRS-5526S 交换机是三层交换机，可以配置多个 IP 地址，配置方法见 4.3 章节。下面以交换机出厂时的情况举例，系统只有 VLAN1 存在。

以下是 Telnet 客户端 Telnet 到交换机的 VLAN1 接口的步骤：

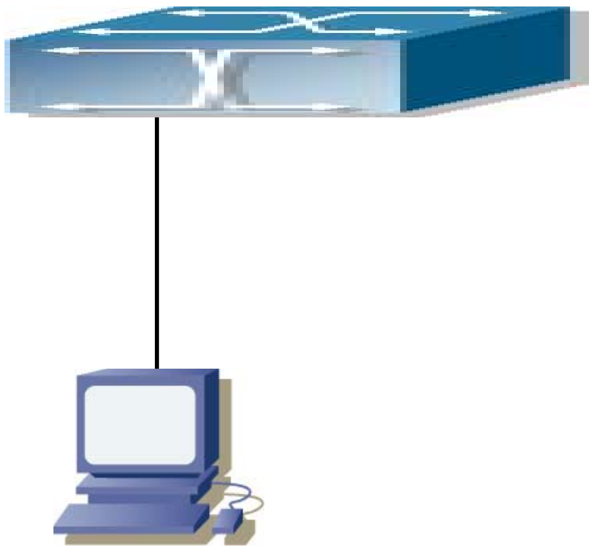


图 4-7 通过 Telnet 管理交换机

第一：配置交换机 IP 地址。

首先配置主机的 IP 地址，要与交换机的 VLAN1 接口 IP 地址在同一个网段。如交换机的 VLAN1 接口 IP 地址为 10.1.128.251，则可以设置主机的 IP 地址为 10.1.128.252。在主机上执行“ping 10.1.128.251”命令，显示是否 ping 通；若 ping 不通，则检查原因。

下面简单介绍配置 DCRS-5526S 的 VLAN1 接口的 IP 地址配置命令，在进行带内管理之前，必须通过带外管理即 Console 口方式配置交换机的 IP 地址，配置命令如下（以后如不特殊说明，所有的交换机配置时的提示符均采用 Switch）：

```
Switch>
Switch>en
Switch#config
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-If-Vlan1)#no shut
```

第二：运行 Telnet 客户端程序。

运行 Windows 自带的 Telnet 客户端程序，并且指定 Telnet 的目的地址。

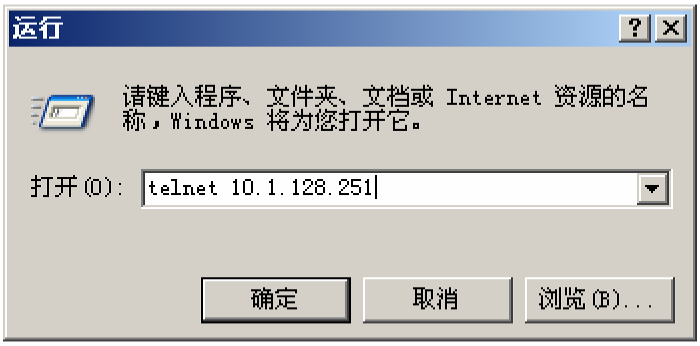


图 4-8　运行 Windows 自带的 telnet 客户端程序

第三：登录交换机。

登录到 Telnet 的配置界面，需要输入正确的登录名和口令，否则交换机将拒绝该 Telnet 用户的访问。该项措施是为了保护交换机免受非授权用户的非法操作。若交换机没有设置授权 Telnet 用户，则任何用户都无法进入交换机的 CLI 配置界面。因此在允许 Telnet 方式配置管理交换机时，必须在 Console 口方式的全局配置模式下使用命令 **telnet-user** ***<user>*** **password {0|7}** ***<password>*** 为交换机设置 Telnet 授权用户和口令。如交换机的授权用户名为 test，口令为明文的 test，设置方式如下：

Switch>en
Switch#config
Switch(Config)#telnet-user test password 0 test

在 Telnet 配置界面上输入正确的登录名和口令，Telnet 用户就可成功的进入到交换机的 CLI 配置界面。Telnet 登录后与通过 Console 口进入后使用的命令完全一致。

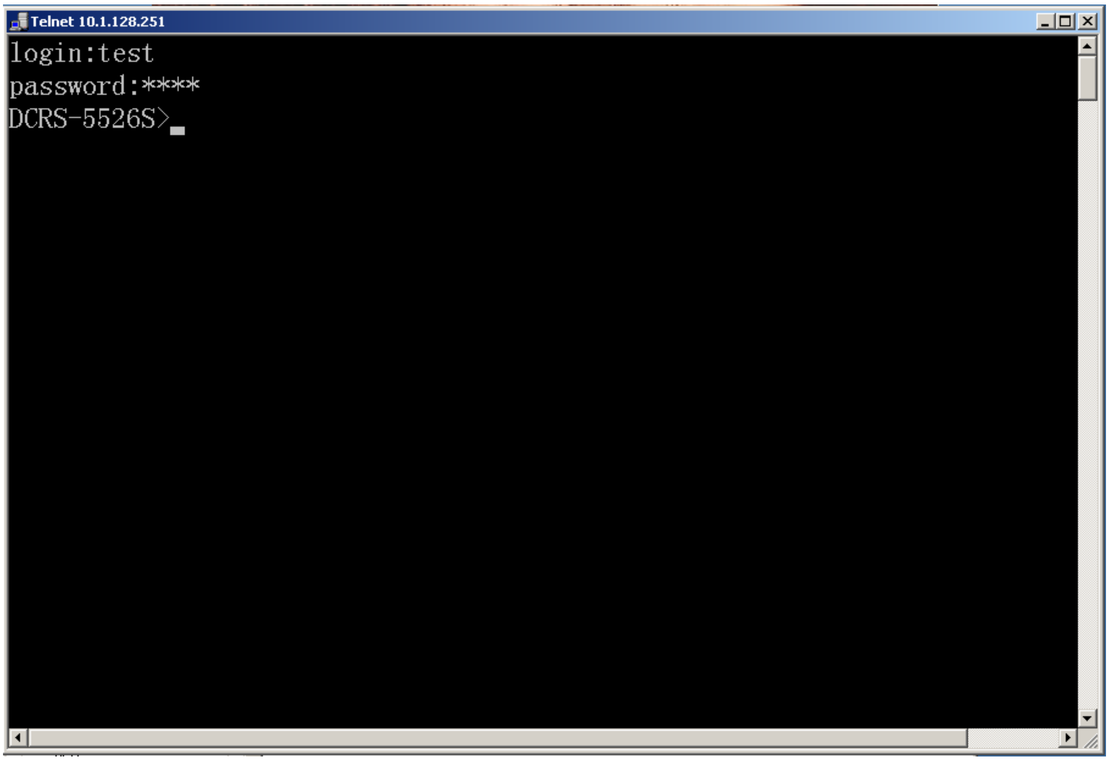


图 4-9 Telnet 配置界面

4.1.2.2通过 HTTP 管理交换机

通过 HTTP 管理交换机要具备的条件：

1) 交换机配置 IP 地址；
2) 作为客户端的主机 IP 地址与其所属交换机的 VLAN 接口的 IP 地址在相同网段；
3) 若不满足 2)，则客户端可以通过路由器等设备到达交换机某个 IP 地址。

与 Telnet 用户登录交换机类似，只要主机能够 ping 通交换机的 IP 地址，并且输入正确的登录口令，该主机就可通过 HTTP 访问交换机。步骤如下：

第一：配置交换机的 IP 地址，并且启动交换机的 HTTP Server 功能。

通过带外管理配置交换机 IP 地址，参见相应章节。

同时 Console 方式下的全局配置模式下使用命令 **ip http server** 启动 HTTP Server 功能，使能 Web 配置。配置如下：

Switch>en
Switch#config
Switch(Config)#ip http server

第二：在配置主机上运行 HTTP 协议。

在主机上打开 Web 浏览器，在地址处输入交换机的 IP 地址，或直接运行 Windows 的 HTTP 协议，比如交换机的 IP 地址为“10.1.128.251”；

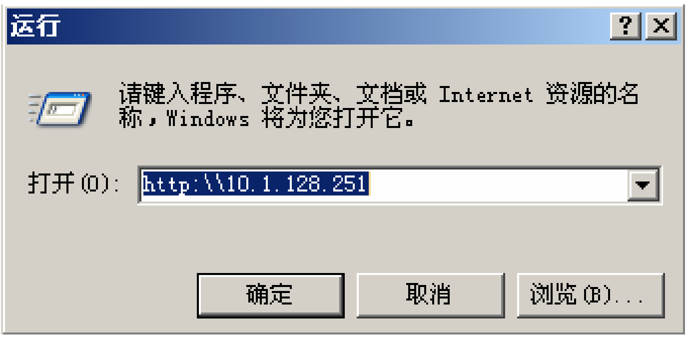


图 4-10 执行 HTTP 协议

第三：Web 访问交换机。

登录到 Web 的配置界面，需要输入正确的登录名和口令，否则交换机将拒绝该 HTTP 访问。该项措施是为了保护交换机免受非授权用户的非法操作。若交换机没有设置授权 Web 用户，则任何用户都无法进入交换机的 Web 配置界面。因此在允许 Web 方式配置管理交换机时，必须在 Console 方式下的全局配置模式下使用命令 **web-user <*user*> password {0|7} <*password*>** 为交换机设置 Web 授权用户和口令。如交换机的授权用户名为 admin，口令为明文的 digital，设置方式如下：

Switch>en

Switch#config

Switch(Config)#web-user admin password 0 digital

下面是 DCRS-5526S 的 Web 配置的登录界面：



图 4-11 DCRS-5526S 的 Web 登录界面

输入正确的用户名和密码，进入交换机的 Web 配置主界面。



图 4-12　DCRS-5526S 的 Web 配置界面

4.1.2.3通过 LinkManager 管理交换机

通过 LinkManager 管理交换机要具备的条件：

1) 交换机配置 IP 地址；
2) 作为 Telnet 客户端的主机 IP 地址与其所属交换机的 VLAN 接口的 IP 地址在相同网段；
3) 若不满足 2），则 Telnet 客户端可以通过路由器等设备到达交换机某个 IP 地址。

安装 LinkManager 网管软件的主机必须能 ping 通交换机的 IP 地址，这样在运行 LinkManager 时，LinkManager 就能找到 DCRS-5526S 设备，并且对其进行可读写的操作。具体如何通过 LinkManager 管理交换机在本手册中不做介绍，请参看《LinkManager 用户手册》。

4.2 管理界面

DCRS-5526S 为用户提供了三种管理界面：CLI（Command Line Interface）命令行界面、Web 界面、LinkManager 网管软件。我们将对 CLI 界面和 Web 界面做详细的介绍，有关 LinkManager 网管软件请参看《LinkManager 用户手册》。

4.2.1 CLI 界面

用户对 CLI 界面并不陌生，前面我们提到的带外管理方式、Telnet 登录到交换机都是通过 CLI 界面对交换机进行配置管理的。

CLI 界面由 Shell 程序提供，它是由一系
列的配置命令组成的，根据这些命令在配置管理交换机时所起的作用不同，Shell 将这些命令分类，不同类别的命令对应着不同的配置模式。下面将介绍交换机的 Shell 的特点：

- 配置模式
- 配置语法
- 快捷键
- 帮助功能
- 对输入的检查
- 支持不完全匹配

4.2.1.1配置模式介绍

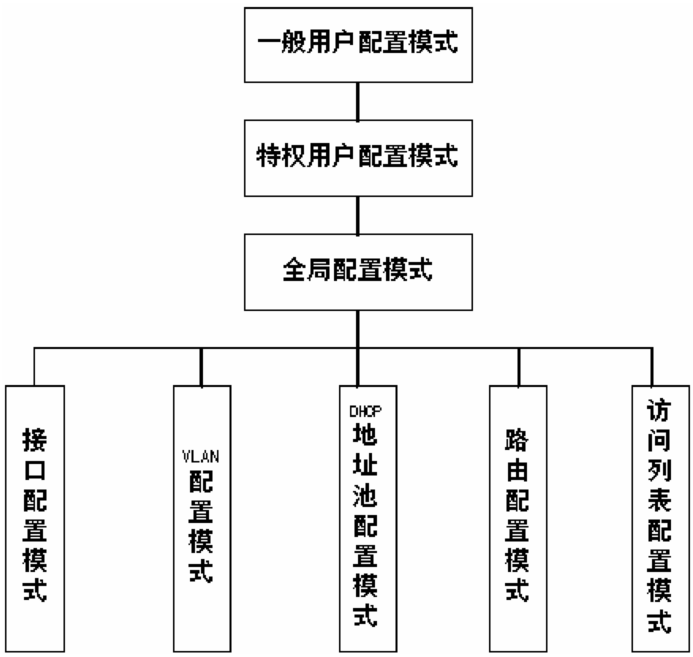


图 4-13　DCRS-5526S 的 Shell 配置模式

4.2.1.1.1 一般用户配置模式

用户进入 CLI 界面，首先进入的就是一般用户配置模式，提示符为"**Switch>**"，符号"**>**"为一般用户配置模式的提示符。当用户从特权用户配置模式使用命令 **exit** 退出时，可以回到一般用户配置模式。

用户在一般用户配置模式下不能对交换机进行任何配置，只能查询交换机的时钟和交换机的版本信息。

4.2.1.1.2 特权用户配置模式

在一般用户配置模式使用 **enable** 命令，如果已经配置了进入特权用户的口令，则输入相应的特权用户口令，即可进入特权用户配置模式"**Switch#**"。当用户从全局模式使用 **exit**

退出时，也可以回到特权用户配置模式。另外 DCRS-5526S 提供“Ctrl+z”的快捷键，使得交换机在任何配置模式（一般用户配置模式除外），都可以退回到特权用户配置模式。

在特权用户配置模式下，用户可以查询交换机配置信息、各个端口的连接情况、收发数据统计等。而且进入特权用户配置模式后，可以进入到全局模式对交换机的各项配置进行修改，因此进行特权用户配置模式必须要设置特权用户口令，防止非特权用户的非法使用，对交换机配置进行恶意修改，造成不必要的损失。

4.2.1.1.3 全局配置模式

进入特权用户配置模式后，只需使用命令 **config**，即可进入全局配置模式“**Switch(Config)#**”。当用户在其他配置模式，如接口配置模式、VLAN 配置模式时，可以使用命令 **exit** 退回到全局配置模式。

在全局配置模式，用户可以对交换机进行全局性的配置，如对 MAC 地址表、端口镜像、创建 VLAN、启动 IGMP Snooping、GVRP、STP 等。用户在全局模式还可通过命令进入到端口对各个端口进行配置。

4.2.1.1.3.1接口配置模式

在全局配置模式，使用命令 **interface** 就可以进入到相应的接口配置模式。DCRS-5526S 操作系统提供了三种端口类型：1.VLAN 接口；2.以太网端口；3.port-channel，因此就有三种接口的配置模式。

接口类型	进入方式	提示符	可执行操作	退出方式
VLAN 接口	在全局配置模式下，输入命令 **interface vlan** ***<Vlan-id>***。	**Switch(Config-If-Vlanx)#**	配置交换机的 IP 地址。	使用 **exit** 命令即可退回全局配置模式。
以太网端口	在全局配置模式下，输入命令 **interface ethernet** ***<interface-list>***。	**Switch(Config-ethernetxx)#**	配置交换机提供的以太网接口的双工模式、速率等。	使用 **exit** 命令即可退回全局配置模式。
port-channel	在全局配置模式下，输入命令 **interface port-channel** ***<port-channel-number>***。	**Switch(Config-if-port-channelx)#**	配置 port-channel 有关的双工模式、速率等。	使用 **exit** 命令即可退回全局配置模式。

4.2.1.1.3.2VLAN 配置模式

在全局配置模式，使用命令 **vlan** **<*vlan-id*>**就可以进入到相应的 VLAN 配置模式。在 VLAN 配置模式，用户可以配置属于本 VLAN 的成员端口。执行 **exit** 命令即可从 VLAN 配置模式退回到全局配置模式。

4.2.1.1.3.3DHCP 地址池配置模式

在全局配置模式下用 **ip dhcp pool** **<*name*>**命令进入到 DHCP 地址池配置模式"**Switch(Config-<*name*>-dhcp)#**"。在 DHCP 地址池配置模式下可以配置 DHCP 地址池的属性。执行"exit"命令即可从 DHCP 地址池配置模式退回到全局配置模式。

4.2.1.1.3.4路由配置模式

路由协议	进入方式	提示符	可执行操作	退出方式
RIP 路由协议	在全局配置模式下输入 **router rip** 命令。	**Switch(Config-Router-Rip)#**	配置 RIP 协议参数。	执行"exit"命令即可退回全局配置模式。
OSPF 路由协议	在全局配置模式下输入 **router ospf** 命令。	**Switch(Config-Router-Ospf)#**	配置 OSPF 协议参数。	执行"exit"命令即可退回全局配置模式。

4.2.1.1.3.5访问列表配置模式

访问列表类型	进入方式	提示符	可执行操作	退出方式
命名标准 IP 访问列表配置模式	在全局配置模式下输入 **ip access-list standard** 命令。	**Switch(Config-Std-Nacl-a)#**	配置标准访问列表配置模式	执行"exit"命令即可退回全局配置模式。
命名扩张 IP 访问列表配置模式	在全局配置模式下输入 **ip access-list extanded** 命令。	**Switch(Config-Ext-Nacl-b)#**	配置扩张访问列表的参数	执行"exit"命令即可退回全局配置模式。

4.2.1.2配置语法

DCRS-5526S 为用户提供了各种各样的配置命令，尽管这些配置命令的形式各不一样，但它们都遵循 DCRS-5526S 配置命令的语法。以下是交换机提供的通用命令格式：

cmdtxt <*variable*> { enum1 | … | enumN } [option]

语法说明：黑体字 **cmdtxt** 表示命令关键字；**<*variable*>**表示参数为变量；**{enum1 | … |**

enumN }表示在参数集 **enum1~enumN** 中必须选一个参数；**[option]**中的“**[ ]**”表示该参数为可选项。在各种命令中还会出现“**< >**”“**{ }**”“**[ ]**”符号的组合使用，如：**[<*variable*>]**，**{enum1 <*variable*>| enum2}**，**[option1 [option2]]** 等等。

下面是几种配置命令语法的具体分析：

- **show version**，没有任何参数，属于只有关键字没有参数的命令，直接输入命令即可；
- **vlan <*vlan-id*>**，输入关键字后，还需要输入相应的参数值；
- **snmp-server community {ro|rw} <*string*>**，出现以下几种输入情况：
  snmp-server community ro <*string*>
  snmp-server community rw <*string*>

4.2.1.3支持快捷键

DCRS-5526S 为方便用户的配置，特别提供了多个快捷键，如上、下、左、右键及删除键 BackSpace 等。如果超级终端不支持上下光标键的识别，可以使用 ctrl+p 和 ctrl+n 来替代。

<table>
<tr><td>按键</td><td colspan="2">功能</td></tr>
<tr><td>删除键 BackSpace</td><td colspan="2">删除光标所在位置的前一个字符，光标前移</td></tr>
<tr><td>上光标键“↑”</td><td colspan="2">显示上一个输入命令。最多可显示最近输入的十个命令</td></tr>
<tr><td>下光标键“↓”</td><td colspan="2">显示下一个输入命令。当使用上光标键回溯到以前输入的命令时，也可以使用下光标键退回到相对与前一个命令的下一个命令</td></tr>
<tr><td>左光标键“←”</td><td>光标向左移动一个位置</td><td rowspan="2">左右键的配合使用，可对已输入的命令做覆盖修改</td></tr>
<tr><td>右光标键“→”</td><td>光标向右移动一个位置</td></tr>
<tr><td>Ctr+p</td><td colspan="2">相对于上光标键“↑”的作用</td></tr>
<tr><td>Ctr+n</td><td colspan="2">相当于下光标键“↓”的作用</td></tr>
<tr><td>Ctr+b</td><td colspan="2">相对于上光标键“←”的作用</td></tr>
<tr><td>Ctr+f</td><td colspan="2">相对于上光标键“→”的作用</td></tr>
<tr><td>Ctr+z</td><td colspan="2">从其他配置模式（一般用户配置模式除外）直接退回到特权用户模式</td></tr>
<tr><td>Ctr+c</td><td colspan="2">打断交换机 ping 或其它正在执行的命令进程</td></tr>
<tr><td>Tab 键</td><td colspan="2">当输入的字符串可以无冲突的表示命令或关键字时，可以使用 Tab 键将其补充成完整的命令或关键字</td></tr>
</table>

4.2.1.4帮助功能

DCRS-5526S 为用户提供了两种方式获取帮助信息，其中一种方式为使用“help”命令，另一种为“？”方式。

帮助	使用方法及功能
Help	在任一命令模式下，输入“help”命令均可获取有关帮助系统的简单描述。
“？”	1. 在任一命令模式下，输入“？”获取该命令模式下的所有命令及其简单描述； 2. 在命令的关键字后，输入以空格分隔的“？”，若该位置是参数，会输出该参数类型、范围等描述；若该位置是关键字，则列出关键字的集

	合及其简单描述；若输出 “<cr>” ，则此命令已输入完整，在该处键入回车即可。 3. 在字符串后紧接着输入“？”，会列出以该字符串开头的所有命令。

4.2.1.5对输入的检查

4.2.1.5.1 成功返回信息

通过键盘输入的所有命令都要经过 Shell 的语法检查。当用户正确输入相应模式下的命令后，且命令执行成功，不会显示信息。

4.2.1.5.2 错误返回信息

输出错误信息	错误原因
Unrecognized command or illegal parameter!	命令不存在，或者参数的范围、类型、格式有错误。
Ambiguous command	根据已有输入可以产生至少两种不同的解释
Invalid command or parameter	命令解析成功，但没有任何有效的参数纪录
This command is not exist in current mode	命令可解析，但当前模式下不能配置该命令
Please configurate precursor command "*" at frist !	当前输入可以被正确解析，但其前导命令尚未配置
syntax error : missing '"' before the end of command line!	输入中使用了引号，但没有成对出现。

4.2.1.6支持不完全匹配

DCRS-5526S 的 Shell 支持不完全匹配的搜索命令和关键字，当输入无冲突的命令或关键字时，Shell 就会正确解析。

例如：

1. 对特权用户配置命令“show interface ethernet 0/01”，只要输入“sh in e 0/01”即可。
2. 对特权用户配置命令 “show running-config”，如果仅输入“sh r”，系统会报“> Ambiguous command!”，因为 Shell 无法区分“show r”是“show rom”命令还是“show running-config”命令，因此必须输入“sh ru”，Shell 才会正确的解析。

4.2.2 Web 界面



图 4-14　DCRS-5526S 的 Web 配置主界面

如上图所示，DCRS-5526S 的 Web 配置界面可分成三部分：上半部分、左下部分、右下部分。

Web 配置界面的上半部分显示 DCRS-5526S 的前面板图，并且通过前面板图上个灯实时显示各端口的连接情况。点击前面板图上的端口在 Web 配置界面的右下部分还可以显示各个端口的流量统计信息。

Web 配置界面的左下部分为主菜单，可以对交换机进行配置、管理、端口监视、交换机的维护等。下面介绍主菜单下的一级子菜单。

主菜单	一级子菜单	描述
交换机配置	路由配置	配置 ARP、RIP 路由配置、IGMP 配置、静态路由配置等。
	ACL 配置	配置标准和扩展 ACL 列表，以及端口 ACL 绑定等。
	VLAN 配置	配置 GVRP、添加和删除 VLAN、端口 VLAN 属性、端口 VLAN 配置、VLAN 接口配置等。
	MAC-Table-Address 相关配置	配置单播地址、及查询 MAC 和删除 MAC。
	MAC 端口绑定相关配置	配置与 MAC 地址绑定的相关参数。
	端口配置	配置带宽控制，物理端口配置，LACP，保护端口，端口镜像及端口信息察看，配置交换机的 IP 地址等。
	交换机信息配置	可查看交换机的版本信息，及配置交换机系统名称，是否打开 HTTP 服务器功能，配置交换机的网关等。
	交换机开关配置	配置交换机的高级配置，有广播抑制，IGMP Snooping、GVRP、RIP 的开关等。

	IGMP Snooping 配置	启动指定 VLAN 的 IGMP Snooping 或 Query 功能，及相关参数的配置。
安全认证配置	Radius 客户端配置	配置 Radius 认证、计费及 Radius Client 的相关参数配置。
	802.1x 配置	配置 802.1x 的相关参数。
QoS 配置	交换机 QoS 配置	配置交换机 QoS 的开关，端口优先级模式，队列出队算法等。
	CoS-to-Queue 映射	配置 CoS 与出口队列的映射关系。
	DSCP-to-Queue 映射	配置 DSCP 与出口队列的映射关系。
	ToS-to-Queue 映射	配置 ToS 与出口队列的映射关系。
	端口配置	配置端口的信任模式。
SNMP 配置管理	SNMP 管理方设置	配置管理站的团体名、访问权限等。
	TRAP 管理方设置	配置 TRAP 管理站的地址、团体名等。
	管理方 IP 地址设置	配置 SNMP 管理站的地址设置。
	SNMP 统计信息	显示 SNMP 统计信息。
	RMON 和 TRAP 配置	配置 RMON 状态和 TRAP 状态。
交换机维护	DHCP 服务器配置	配置与 DHCP 服务器相关的参数。
	TFTP 服务	配置 TFTP 客户端服务和 TFTP 服务器端服务。
	FTP 服务	配置 FTP 客户端服务和 FTP 服务器端服务。
	Telnet 服务器端服务	配置交换机作为 Telnet 服务器时授权访问的 Telnet 用户名和口令及 Telnet 安全 IP 地址。
	Web 服务器用户管理	配置交换机作为 HTTP 服务器时授权访问的 Web 用户名和口令。
	显示 Flash 文件信息	显示系统中保存文件的类型及长度。
	下次以出厂初始设置启动	恢复出厂配置。**注意：**用户在选择下次以出厂初始设置启动时必须要**保存配置**后才选择重启，否则重启后不恢复出厂设置。
	保存配置	进行配置保留操作。
	退出配置	执行退出配置的操作。
	重新启动	执行重启交换机的操作。
帮助信息		显示帮助信息。

Web 配置界面的右下部分是显示及与用户交互的部分。当用户点击上半部分或者左下部分时，在 Web 配置界面的右下部分就显示出相关菜单（子菜单）的配置界面，用户可以根据自己的需求配置交换机。具体配置界面中出现的参数可参见相关章节的配置介绍。

使用 Web 界面配置时需要注意以下几点：

注意点一：

请用 IE6.0 以上版本的浏览器，800*600 分辨率，且必须开启 JavaScript。

注意点二：

为确保 CGI 程序执行的正确性，务必保证浏览器每次是从服务器读取新内容，而不是系统缓存中读取内容。以下是如何保证浏览器每次都从服务器读取新内部的具体操作：在网页菜单中选择工具（T）→Internet 选项；或者在桌面使用鼠标右键点击 IE 浏览器进入属性，进入如下配置界面。

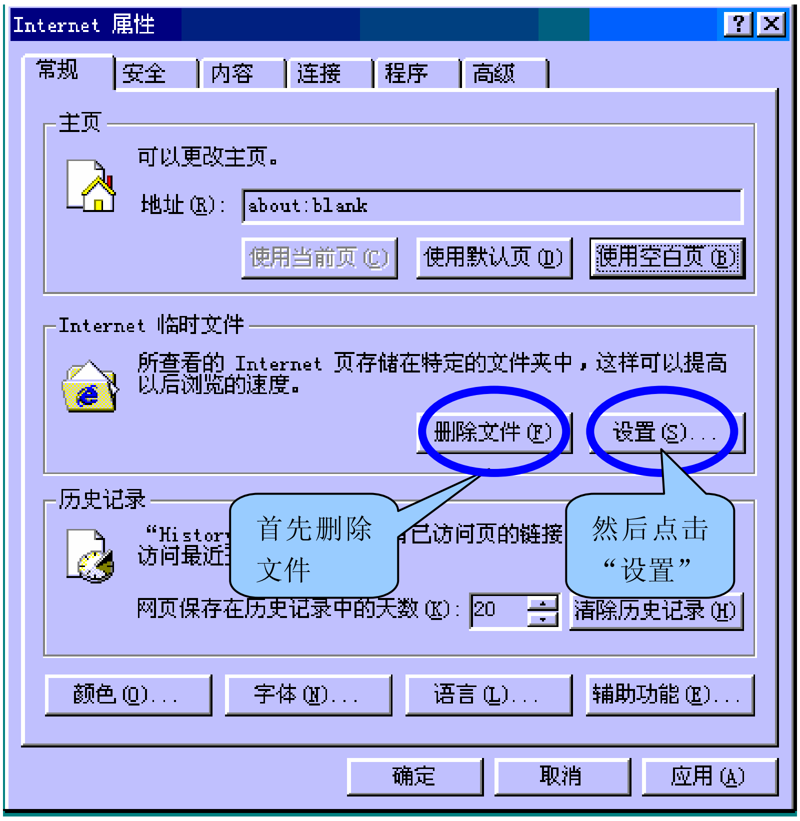


图 4-15 Internet 属性配置

首先点击“删除文件（F）”，然后点击“设置（S）”，进入配置界面如下图。

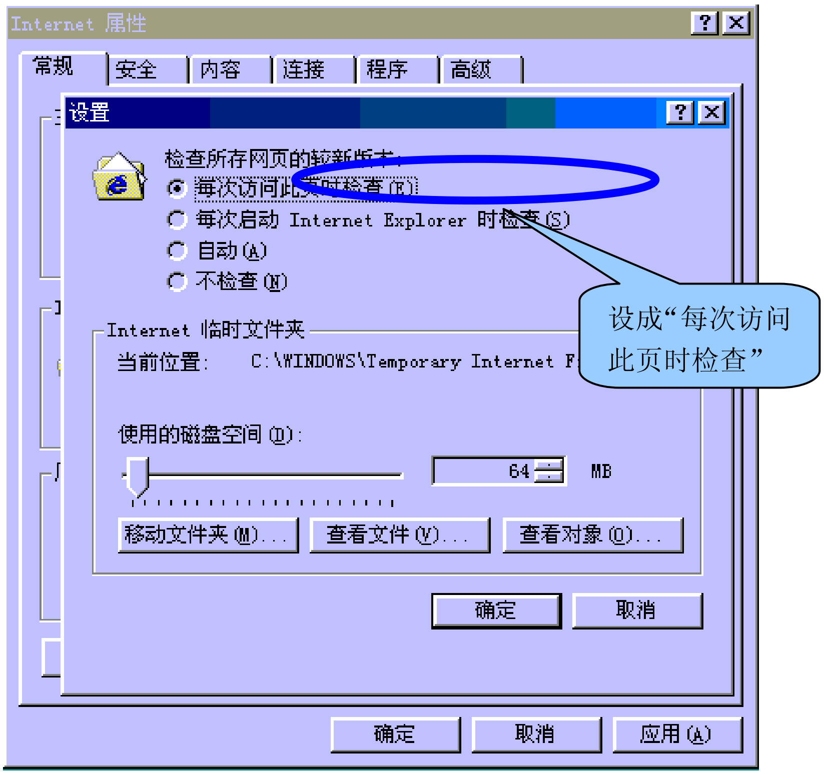


图 4-16 进入"设置"界面

选中"每次访问此页时检查"。

第5章 交换机基本配置

5.1 基本配置命令

交换机的基本配置包括从进入和退出特权用户模式的命令、进入和退出接口配置模式的命令、设置及显示交换机的时钟、显示交换机的系统版本信息等。

注意:

缺省情况下，交换机的主机名和命令行界面提示符与交换机的型号相一致，在本章中以“Switch”字样来表示通用的命令行提示符。

5.1.1 clock set

命令：**clock set <*HH:MM:SS*> <*YYYY/MM/DD*>**
功能：设置系统日期和时钟。
参数：**<*HH:MM:SS* >**为当前时钟，***HH*** 取值范围为 0~23，***MM*** 和 ***SS*** 取值范围为 0~59；**< *YYYY/MM/DD* >**为当前年、月和日，***YYYY*** 取值范围为 2000~2100，***MM*** 取值范围为 1~12，***DD*** 取值范围为 1~31。
命令模式：特权用户配置模式
缺省情况：系统启动时缺省为 2001 年 1 月 1 日 0：0：0。
使用指南：交换机在断电后不能继续计时，因此在要求使用确切时间的应用环境中，必须先设定交换机当前的日期和时间。
举例：设置交换机当前日期为 2002 年 8 月 1 日 23 时 0 分 0 秒。
Switch#clock set 23:0:0 2002.8.1
相关命令：**show clock**

5.1.2 config

命令：**config [terminal]**
功能：从特权用户配置模式进入到全局配置模式。
参数：**[terminal]**表示进行终端配置。
命令模式：特权用户配置模式
举例：
Switch#config

5.1.3 exec timeout

命令：exec timeout <*minutes* >
功能：设置退出特权用户配置模式超时时间。
参数：< *minute* >为时间值，单位为分钟，取值范围为 0~300。
命令模式：全局配置模式。
缺省情况：系统缺省为 5 分钟。
使用指南：为确保交换机使用的安全性，防止非法用户的恶意操作，当特权用户在做完最后一项配置后，开始计时，到达设置时间值时，系统就自动退出特权用户配置模式。用户如果想再次进入特权用户配置模式，需要再次输入特权用户密码和口令。当设置超时时间为 0 时，停止超时计时器。
举例：设置交换机退出特权用户配置模式的超时时间为 6 分钟。
Switch(Config)#exec timeout 6↵

5.1.4 exit

命令：exit
功能：从当前模式退出，进入上一个模式，如在全局配置模式使用本命令退回到特权用户配置模式，在特权用户配置模式使用本命令退回到一般用户配置模式等。
命令模式：各种配置模式
举例：
Switch#exit
Switch>

5.1.5 help

命令：help
功能：输出有关命令解释器帮助系统的简单描述。
命令模式：各种配置模式
使用指南：交换机提供随时随地的在线帮助，help 命令则显示关于整个帮助体系的信息，包括完全帮助和部分帮助，用户可以随时随地键入？获取在线帮助。
举例：

```
Switch>help
  enable                  -- Enable Privileged mode
  exit                    -- Exit telnet session
  help                    -- help
  show                    -- Show running system information
```

5.1.6 ip host

命令：**ip host <*hostname*> <*ip_addr*>**
no ip host <*hostname*>
功能：设置主机与 IP 地址映射关系；本命令的 no 操作为删除该项映射关系。
参数：**<*hostname*>**为主机名称，最长不超过 30 个字符；**<*ip_addr*>**为主机名相应 IP 地址，点分十进制格式。
命令模式：全局配置模式
使用指南：设置一个确定的主机和 IP 地址的对应关系，可用于如"**ping <host>**"等命令中。
举例：设置主机名为 beijing 的主机的 IP 地址为 200.121.1.1
Switch(Config)#ip host beijing 200.121.1.1
相关命令：**telnet**、**ping**、**traceroute**

5.1.7 ip http server

命令：**ip http server**
no ip http server
功能：使能 Web 配置；本命令的 no 操作为关闭 Web 配置。
命令模式：全局配置模式
使用指南：Web 配置是给用户提供一个以 HTTP 方式配置的界面。Web 配置的优点是配置直观、形象，容易理解。本命令的作用相当于在 Setup 配置模式的主菜单中选择[2]，进行 Web Server 的配置。
举例：打开 Web Server 功能，使能 Web 配置。
Switch(Config)#ip http server
相关命令：**web-user**

5.1.8 hostname

命令：**hostname <*hostname*>**
功能：设置交换机命令行界面的提示符。
参数：**<*hostname*>**为提示符的字符串，最长不超过 15 个字符。
命令模式：全局配置模式
缺省情况：系统缺省提示符和交换机型号有关。
使用指南：通过本命令用户可以根据实际情况设置交换机命令行的提示符。
举例：设置提示符为 Test。
Switch(Config)#hostname Test
Test(config)#

5.1.9 reload

命令：**reload**
功能：热启动交换机。
命令模式：特权用户配置模式

使用指南：用户可以通过本命令，在不关闭电
源的情况下，重新启动交换机。

5.1.10 set default

命令：**set default**
功能：恢复交换机的出厂设置。
命令模式：特权用户配置模式
使用指南：恢复交换机的出厂设置，即用户对交换机做的所有配置都消失，用户重新启动交换机后，出现的提示与交换机首次上电一样。
注意：配置本命令后，必须执行 **write** 命令，进行配置保留后**重启交换机**即可使交换机恢复到出厂设置。
举例：
Switch#set default
Are you sure? [Y/N] = y
Switch#write
Switch#reload

5.1.11 setup

命令：**setup**
功能：进入交换机的 Setup 配置模式。
命令模式：特权用户配置模式
使用指南：在 Setup 配置模式下用户可进行 IP 地址、Web 服务等的配置。

5.1.12 language

命令：**language {chinese|english}**
功能：设置显示的帮助信息的语言类型。
参数：**chinese** 为中文显示；**english** 为英文显示。
命令模式：特权用户配置模式
缺省情况：系统缺省英文显示。
使用指南：用户可根据自己的喜好选择语言类型。系统若重启后，帮助显示信息恢复为英文显示。

5.1.13 web-user

命令：**web-user <*username*> password {0|7} <*password*>**
no web-user <*username*>
功能：设置 Web 客户端的用户名及口令；本命令的 no 操作为删除该 Web 客户。
参数：**<*username*>**为 Web 访问的授权用户名，最长不超过 16 个字符；**<*password*>**为登

录口令，最长不超过 8 个字符；**0|7** 分别表示
口令不加密显示和加密显示。
命令模式：全局配置模式
使用指南：为了防止非授权用户的 Web 访问，管理员可以使用本命令配置 Web 访问的授权用户及口令。
举例：设置一个名为 Admin 的 Web 访问用户，密码为 switch。
Switch(Config)#web-user Admin password 0 switch
相关命令：**ip http server**

5.1.14 write

命令：write
功能：将当前运行时配置参数保存到 Flash Memory。
命令模式：特权用户配置模式
使用指南：当完成一组配置，并且已经达到预定功能，应将当前配置保存到 Flash 中，以便因不慎关机或断电时，系统可以自动恢复到原先保存的配置。相当于 **copy running-config startup-config** 命令

5.2 维护和调试命令

当用户配置交换机时，需要查看各项配置是否配置正确，交换机是否符合期望工作正常；或者当网络出现了故障，用户需要诊断故障，DCRS-5526S 为此提供了 ping、telnet、show、debug 等多种调试命令，帮助用户查看系统配置、运行状态，找到故障原因。

5.2.1ping

命令：ping [<*ip-addr*>|<hostname>]
功能：交换机向远端设备发 ICMP 请求包，检测交换机与远端设备之间是否可达。
参数：<*ip-addr*>为要 ping 的目的主机的 IP 地址，点分十进制格式。
<hostname>为要 ping 的目的主机的主机名，为字母开头的数字字母组成的字符串，中间不可有空格，字符串长度为（1-30）。
缺省情况：发 5 个 ICMP 请求包；包大小为 56 bytes；超时时间为 2 秒。
命令模式：特权用户配置模式
使用指南：当用户输入 ping 命令后，直接回车，系统提供给用户一种交互式的配置方式，用户可以自己定义 ping 的各项参数值。
举例：
例 1：使用 ping 程序的缺省参数。
Switch#ping 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.
...!!

Success rate is 40 percent (2/5), round-trip
min/avg/max = 0/0/0 ms
上面的例子表示，交换机 ping 某一 IP 地址为 10.1.128.160 的设备，前三个 ICMP 请求包在缺省超时时间 2 秒内没有收到相应的 ICMP 回应包，即没有 ping 通，而后两个包 ping 通了，成功率为 40%。交换机用"."表示 ping 失败，链路不可达；用"！"表示 ping 成功，链路可达。
例 2：使用 ping 程序提供的手段修改 ping 参数。
Switch#ping ↵
protocol [IP]：　↵
Target IP address：10.1.128.160↵
Repeat count [5]：100 ↵
Datagram size in byte [56]：1000 ↵
Timeout in milli-seconds [2000]：500 ↵
Extended commands [n]：n ↵

显示信息	解释
protocol [IP]：	选择 IP 协议的 Ping；
Target IP address：	目标设备的 IP 地址；
Repeat count [5]	发包的数目，默认为 5；
Datagram size in byte [56]	ICMP 包的大小，默认为 56；
Timeout in milli-seconds [2000]：	超时时间，单位为毫秒，默认为 2 秒；
Extended commands [n]：	是否改变需要其他的选项；

5.2.2Telnet

5.2.2.1Telnet 简介

Telnet 远程登录是一个简单的远程终端协议。用户用 Telnet 就可在其所在地通告 TCP 连接注册（即登录）到远程的另一个主机上（使用 IP 地址或主机名）。Telnet 能把用户的击键传到远程的主机，同时也能把远程主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户的感觉是键盘和显示器是直接连接在远程主机上。

Telnet 使用客户－服务器模式，在本地的系统为 Telnet 客户端，远程主机为 Telnet 服务器。DCRS-5526S 既可以作为 Telnet 服务器也可以作为 Telnet 客户端。

当 DCRS-5526S 作为 Telnet 服务器时，用户可以通过 Windows 或其他操作系统自带的 Telnet 客户端软件，Telnet 登录到 DCRS-5526S，就如前面介绍带内管理章节中介绍的一样。DCRS-5526S 作为 Telnet 服务器时最多可以同时与 5 个 Telnet 客户端建立 TCP 连接。

当作为 Telnet 客户端时，在交换机的特权用户配置模式下使用 telnet 命令即可登录到其他远端主机。DCRS-5526S 作为 Telnet 客户端时只能与一个远程主机建立 TCP 连接，如果想与另一个远程主机建立连接，则必须先断开与上一个远程主机的 TCP 连接。

5.2.2.2Telnet 任务序列

1. 配置 Telnet 服务器
2. 交换机 Telnet 登录到远程主机

1. 配置 Telnet 服务器

命令	解释
全局配置模式	
telnet-server enable **no telnet-server enable**	打开交换机的 Telnet 服务器功能；本命令的 no 操作为关闭 Telnet 服务器功能。
telnet-user ***<user-name>*** **password {0|7}** ***<password>*** **no telnet-user** ***<user-name>***	配置 Telnet 登录到交换机的用户名和口令；本命令的 no 操作为删除授权 Telnet 用户。
telnet-server securityip ***<ip-addr>*** **no telnet-server securityip** ***<ip-addr>***	配置 Tenet 登录到交换机的安全 IP 地址；本命令的 no 操作为删除授权 Telnet 安全地址。
authentication login {local|radius|local radius|radius local} **no authentication login**	配置远程登录验证方式
特权模式	
Monitor **no monitor**	使登录到交换机的 Tenet 客户端显示调试信息；本命令的 no 操作为关闭 Telnet 客户端显示调试信息的功能。

2. 交换机 Telnet 登录到远程主机

命令	解释
特权模式	
telnet [<*ip-addr*>] [<*port*>]	使用交换机提供的 Telnet 客户端登录到远程主机。

5.2.2.3Telnet 命令介绍

5.2.2.3.1 authentication login

命令：authentication login {local | radius | local radius | radius local}
no authentication login

功能：配置 Telnet Server 对远程登录用户的密码验证方式和优先级；该命令的 no 命令恢复缺省验证方式。

缺省情况：缺省登陆验证方式为 local。

命令模式：全局配置模式

使用指南：当采用组合验证方式时，在最前面的验证方式优先级最高，并依次递减；如果高

优先级方式验证通过，则直接允许用户登陆，
并忽略后面的验证方式。需要注意的是：只要有一种验证方式验证通过，用户就可以登陆。当使用 radius 验证时，必须使能 AAA 功能并配置 radius 服务器。
举例：配置远程登录的验证方式为 radius。
Switch(Config)#authentication login radius
相关命令：
aaa enable
radius-server authentication host

5.2.2.3.2 monitor

命令：**monitor**
no monitor
功能：使能 Telnet 客户端的显示调试信息，同时关闭 Console 端显示调试信息的功能；本命令的 no 操作为关闭 Telnet 客户端显示调试信息的功能，恢复 Console 端显示调试信息的功能。
命令模式：特权用户配置模式
使用指南：通常 Telnet 客户端在访问交换机时，如果打开 Debug 调试信息，Debug 信息不会显示在 Telnet 界面上，而是显示在 Console 口连接的超级终端上；使用本命令可使调试信息显示在指定的 Telnet 终端的界面上而不是 Console 或者其他 Telnet 终端界面上。monitor 只在 telnet 终端下有效。
举例：使能 Telnet 客户端显示调试信息。
Switch#monitor
相关命令：**telnet-user**

5.2.2.3.3 telnet

命令：**telnet [<*ip-addr*>] [<*port*>]**
功能：以 Telnet 方式登录到 IP 地址为**<*ip-addr*>**的远程主机。
参数：**<*ip-addr*>**为远端主机的 IP 地址，点分十进制格式；**<*port*>**为端口号，取值范围 0~65535。
命令模式：特权用户配置模式
使用指南：本命令是交换机作为 Telnet 客户端时使用的，用户通过本命令登录远程主机进行配置。当交换机作为 Telnet 客户端时，只能与一个远程主机建立 TCP 连接，如果想与另一个远程主机建立连接，则必须先断开与上一个远程主机的 TCP 连接。断开与远程主机的连接可以使用快捷键"CTRL+ | "。
直接输入关键字 **Telnet** 后面不加任何参数，用户将进入 Telnet 配置模式。
举例：交换机 Telnet 到 IP 地址为 20.1.1.1 的远程路由器 DCR。
Switch#telnet 20.1.1.1 23
Trying 20.1.1.1...
Service port is 23
Connected to 20.1.1.1
login:123
password:***

DCR>

5.2.2.3.4 telnet-server enable

命令：telnet-server enable

no telnet-server enable

功能：打开交换机的 Telet 服务器功能；本命令的 no 操作为关闭交换机的 Telnet 服务器功能。

缺省情况：系统缺省打开 Telnet 服务器功能。

命令模式：全局配置模式

使用指南：该命令只能在 Console 下使用，管理员使用本命令允许或拒绝 Telnet 客户端登录到交换机。

举例：关闭交换机的 Telnet 服务器功能。

Switch(Config)#no telnet-server enable

5.2.2.3.5 telnet-server securityip

命令：telnet-server securityip <*ip-addr*>

no telnet-server securityip <*ip-addr*>

功能：配置交换机作为 Telnet 服务器允许登录的 Telnet 客户端的安全 IP 地址；本命令的 no 操作为删除指定的 Telnet 客户端的安全 IP 地址。

参数：<*ip-addr*> 可以访问本交换机的安全 IP 地址，点分十进制格式。

缺省情况：系统缺省不配置任何安全 IP 地址。

命令模式：全局模式

使用指南：没有配置安全 IP 地址前，不限制登录交换机的 Telnet 客户端的 IP 地址；配置安全 IP 地址后，只有安全 IP 地址的主机才能够 Telnet 到交换机进行配置。交换机允许配置多个安全 IP 地址。

举例：设置 192.168.1.21 为安全 IP 地址。

Switch(Config)#telnet-server securityip 192.168.1.21

5.2.2.3.6 telnet-user

命令：telnet-user <*username*> password {0|7} <*password*>

no telnet-user <*username*>

功能：设置 Telnet 客户端的用户名及口令；本命令的 no 操作为删除该 Telnet 用户。

参数：<*username*>为 Telnet 客户端用户名，最长不超过 16 个字符；**<*password*>**为登录口令，最长不超过 8 个字符；**0|7** 分别表示口令不加密显示和加密显示。

命令模式：全局配置模式

缺省情况：系统缺省没有设置 Telnet 客户端的用户名及口令。

使用指南：本命令是交换机作为 Telnet 服务器时使用的，用户通过本命令设置授权的 Telnet 客户端。若没有设置授权的 Telnet 客户端，任何 Telnet 客户端都不能通过 Telnet 配置交换机。交换机作为 Telnet 服务器时，最多允许同时与 5 个 Telnet 客户端建立 TCP 连接。

举例：设置一个名为 Antony 的 Telnet 客户端用户，密码为 switch。

Switch(Config)#telnet-user Antony password 0 switch

5.2.3SSH

5.2.3.1SSH 简介

SSH 是 Secure Shell 安全外壳的简写，它建立在可靠的 TCP/IP 等通信协议之上，通过 SSH 服务器和 SSH 客户端软件之间的密钥交换，身份认证，加密等算法的协商，在它们之间建立一条安全的传输信息的通道，保证双方交互的信息不能被任何第三方截取和破译，从而最大限度的保证了对实现 SSH 服务器功能的交换机的配置和管理。目前交换机上实现的是符合 SSH2.0 协议规定的 SSH 服务器。支持 SSH2.0 标准的终端软件如 SSH Secure Client，putty 等可以利用 SSH2.0 协议，远程登陆交换机上的 SSH 服务器，实现对该交换机的安全的配置和管理。

目前 SSH 服务器支持客户端软件对主机的 RSA 公钥认证，支持协议规定的 3DES 加密算法，以及 SSH 服务器对 SSH 用户的密码认证等。

5.2.3.2SSH 服务器配置任务序列

1. SSH 服务器配置

命令	解释
全局配置模式	
ssh-server enable **no ssh-server enable**	打开交换机的 SSH 服务器功能；本命令的 no 操作为关闭 SSH 服务器功能。
ssh-user <*user-name*> password {0|7} <*password*> **no ssh-user <*user-name*>**	配置 SSH 客户端软件登录到交换机的用户名和口令；本命令的 no 操作为删除授权 SSH 用户。
ssh-server timeout <*timeout*> **no ssh-server timeout**	设置 SSH 认证超时时间；本命令的 no 操作恢复缺省的 SSH 认证超时时间。
ssh-server authentication-retires < *authentication-retires*> **no ssh-server authentication-retries**	设置 SSH 认证重试次数；本命令的 no 操作恢复缺省的 SSH 认证重试次数。
ssh-server host-key create rsa modulus <*moduls*>	生成新的 SSH 服务器的 RSA 主机密钥对。
特权模式	
monitor **no monitor**	使登录到交换机的 SSH 客户端显示调试信息；本命令的 no 操作为关闭 SSH 客户端显示调试信息的功能。

5.2.3.3 SSH 配置命令

5.2.3.3.1 ssh-server enable

命令：**ssh-server enable**

no ssh-server enable

功能：打开交换机的 SSH 服务器功能；本命令的 no 操作为关闭交换机的 SSH 服务器功能。
缺省情况：系统缺省关闭 SSH 服务器功能。
命令模式：全局配置模式
使用指南：如果需要 SSH 客户端登录到该交换机，需要交换机配置 SSH 用户，且打开 SSH 服务，然后 SSH 客户端才能正确登录 SSH 服务器，对交换机进行配置管理。
举例：打开交换机的 SSH 服务器功能。
Switch(Config)#ssh-server enable

5.2.3.3.2 ssh-user

命令：ssh-user <*username*> password {0|7} <*password*>
no ssh-user <*username*>
功能：设置 SSH 客户端的用户名及口令；本命令的 no 操作为删除该 SSH 用户。
参数：<*username*>为 SSH 客户端用户名，最长不超过 16 个字符；**<*password*>**为登录口令，最长不超过 8 个字符；**0|7** 分别表示口令不加密显示和加密显示。
命令模式：全局配置模式
缺省情况：系统缺省没有设置 SSH 客户端的用户名及口令。
使用指南：用户通过本命令设置授权的 SSH 客户端。任何没有授权的 SSH 客户端都不能通过 SSH 登录和配置交换机。交换机作为 SSH 服务器时，最多设置 3 个用户，最多允许同时与 3 个 SSH 客户端建立 TCP 连接。
举例：设置一个名为 switch 的 SSH 客户端用户，密码为 switch。
Switch(Config)#ssh-user switch password 0 switch

5.2.3.3.3 ssh-server timeout

命令：ssh-server timeout <*timeout*>
no ssh-server timeout
功能：设置 SSH 客户端的验证超时时间；本命令的 no 操作为恢复缺省的超时时间。
参数：<*timeout*>为超时时间，范围为 10-600 秒。
命令模式：全局配置模式
缺省情况：系统缺省设置 SSH 客户端验证超时时间为 180 秒。
使用指南：本命令设置 SSH 客户端验证超时时间，系统缺省的超时时间为 180 秒。
举例：设置 SSH 客户端验证超时时间为 240 秒。
Switch(Config)#ssh-server timeout 240

5.2.3.3.4 ssh-server authentication-retries

命令：ssh-server authentication-retries < authentication-retries >
no ssh-server authentication-retries
功能：设置 SSH 客户端的验证重试次数；本命令的 no 操作为恢复缺省的重试次数。
参数：< authentication-retries >为验证重试次数，范围为 1-10 次。
缺省情况：系统设置的 SSH 验证重试次数为 3 次。
命令模式：全局配置模式

使用指南：

举例：设置 SSH 客户端的验证重试次数为 5 次。

Switch(Config)#ssh-server authentication-retries 5

5.2.3.3.5 ssh-server host-key create rsa

命令：ssh-server host-key create rsa [modulus < modulus >]

功能：为 SSH 服务器创建新的 RSA 主机密钥。

参数：modulus 为计算主机密钥所使用的模，范围为 768-2048，缺省为 1024。

缺省情况：系统缺省使用 ssh-server 服务第一次启动时自动生成的密钥。

命令模式：全局配置模式

使用指南：使用该命令可以创建新的主机密钥，然后 SSH 客户端登录该服务时，使用新生成的密钥进行主机认证。在生成新的密钥，并用 write 命令配置保留后，系统以后都使用该密钥进行主机认证。由于密钥计算需要较长时间，而且有个别客户端软件不兼容利用模 2048 计算出来的密钥，所以从安全效率和兼容性上考虑，建议采用缺省的模 1024 生成主机密钥。

举例：生成新的主机密钥。

Switch(Config)#ssh-server host-key create rsa

5.2.3.3.6 monitor

命令：monitor

no monitor

功能：使能 SSH 客户端的显示调试信息，同时关闭 Console 端显示调试信息的功能；本命令的 no 操作为关闭 SSH 客户端显示调试信息的功能，恢复 Console 端显示调试信息的功能。

命令模式：特权用户配置模式

使用指南：通常 SSH 客户端在访问交换机时，如果打开 Debug 调试信息，Debug 信息不会显示在 SSH 界面上，而是显示在 Console 口连接的超级终端上；使用本命令可使调试信息显示在指定的 SSH 终端的界面上而不是 Console 或者其他 Telnet 或者 SSH 终端界面上。

举例：使能 SSH 客户端显示调试信息。

Switch#monitor

相关命令：ssh-user

5.2.3.4SSH 服务器配置举例

案例 1：

组网需求：交换机端运行 SSH 服务器，终端运行支持 SSH2.0 标准的客户端软件如 Secure shell client 和 putty 等。客户端使用用户名和密码方式登录交换机。

交换机首先配置本地的地址，然后增加 SSH 用户，启动 SSH 服务，这样 SSH2.0 客户端软件就可以利用交换机配置的用户名和密码远程登录配置 SSH 服务的交换机了。

Switch(Config)#interface vlan 1

Switch(Config-Vlan-1)#ip address 100.100.100.200 255.255.255.0

Switch(Config-Vlan-1)#exit

Switch(Config)#ssh-user test password 0 test

Switch(Config)#ssh-server enable

5.2.3.5SSH 监测和调试命令

5.2.3.5.1 show ssh-user

命令：**show ssh-user**
功能：显示所有已配置的 SSH 用户名。
命令模式：特权用户配置模式
举例：
Switch#show ssh-user
test
相关命令：**ssh-user**

5.2.3.5.2 show ssh-server

命令：**show ssh-server**
功能：显示 SSH 服务器的状态是打开还是关闭,以及已经登录的 SSH 用户信息。
命令模式：特权用户配置模式
举例：
Switch#show ssh-server
ssh-server is enabled

connection	version	state	user name
1	2.0	session started	test

相关命令：**ssh-server enable，no ssh-server enable**

5.2.3.5.3 debug ssh-server

命令：**debug ssh-server**
no debug ssh-server
功能：打开 SSH 服务器的调试信息；本命令的 no 操作为关闭 SSH 服务器的调试信息。
缺省情况：缺省调试开关是关闭的。
命令模式：特权用户配置模式

5.2.4traceroute

命令：**traceroute {<*ip-addr*> | host <*hostname*> }[hops <*hops*>] [timeout <*timeout*>]**
功能：本命令用于测试数据包从发送设备到目的地设备所经过的网关，检测网络是否可达，定位网络故障所在。
参数：**<*ip-addr*>**是目的主机的 IP 地址，点分十进制格式；**<*hostname*>**是为远端主机的主机名；**<*hops*>**为 Traceroute 的最大经过的网关数目；**<*timeout*>**为数据包超时时间，单位

为毫秒，取值范围 100~10000。
缺省情况：数据包最多经过的网关数目缺省为 16，超时时间为 2000 毫秒。
命令模式：特权用户配置模式
使用指南：Traceroute 一般用于定位目的网络不可达时的故障所在。
相关命令：ip host

5.2.5show

show 命令是用来显示交换机的系统信息、端口信息、协议运行情况等。本部分介绍交换机的显示系统信息的 show 命令，其它的 show 命令会在相关章节有介绍。

5.2.5.1 show clock

命令：show clock
功能：显示系统当前的时钟。
命令模式：特权用户配置模式
使用指南：用户可以通过查看系统日期和时钟，发现如果系统时间有误，可及时调整。
举例：
Switch#show clock
Current time is TUE AUG 22 11：00：01 2002
相关命令：clock set

5.2.5.2 show debugging

命令：show debugging
功能：显示调试开关的状态。
使用指南：如果用户需要查看当前打开了哪些调试开关，可以执行 **show debugging** 命令。
命令模式：特权用户配置模式
举例：查看当前打开的调试开关。
Switch#show debugging
STP:
        Stp input packet debugging is on
        Stp output packet debugging is on
        Stp basic debugging is on
Switch#
相关命令：debug

5.2.5.3 show flash

命令：show flash
功能：显示保存在 flash 中的文件及大小。
命令模式：特权用户配置模式

举例：查看 flash 中文件及大小。

Switch#show flash

file name   file length

nos.img   1122380 bytes

startup-config   1061 bytes

running-config   1061 bytes

Switch#

5.2.5.4 show history

命令：show history

功能：显示用户最近输入的历史命令。

命令模式：特权用户配置模式

使用指南：系统最多保存 10 条用户最近输入的历史命令，用户在输入命令时可以用上下光标键或其等价键（ctrl+p 和 ctrl+n）来访问历史命令。

举例：

Switch#show history

enable

config

interface ethernet 0/0/3

enable

show flash

show ftp

5.2.5.5 show memory

命令：show memory

功能：显示指定内存区域的内容。

命令模式：特权用户配置模式

使用指南：本命令用于调试交换机。命令以交互的方式提示用户输入所需显示信息的内存首地址和输出字(word)数。显示信息分三个部分：地址、信息的十六进制显示及字符显示。

举例：

Switch#show memory

start address : 0x2100

number of words[64]:

```
002100:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002110:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002120:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002130:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002140:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002150:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002160:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
002170:   0000 0000 0000 0000   0000 0000 0000 0000    *................*
```

5.2.5.6 show rom

命令：**show rom**
功能：显示启动文件及大小。
命令模式：特权用户配置模式
举例：查看启动文件信息。
Switch#sh rom
file name   file length
nos.rom   170992 bytes

5.2.5.7 show running-config

命令：**show running-config**
功能：显示当前运行状态下生效的交换机参数配置。
缺省情况：对于正在生效的配置参数，如果与缺省工作参数相同，则不显示。
命令模式：特权用户配置模式
使用指南：当用户完成一组配置后，需要验证是否配置正确，则可以执行 show running-config 命令来查看当前生效的参数。
举例：
Switch#show running-config

5.2.5.8 show startup-config

命令：**show startup-config**
功能：显示当前运行状态下写在 Flash Memory 中的交换机参数配置，通常也是交换机下次上电启动时所用的配置文件。
缺省情况：从 Flash 中读出的配置参数，如果与缺省工作参数相同，则不显示。
命令模式：特权用户配置模式
使用指南：**show running-config** 和 **show startup-config** 命令的区别在于，当用户完成一组配置之后，通过 **show running-config** 可以看到配置增加了，而通过 **show startup-config** 看不到配置的变化。但若用户通过 **write** 命令，将当前生效的配置保存到 Flash Memory 中时，**show running-config** 的显示与 **show startup-config** 的显示结果一致。

5.2.5.9 show switchport interface

命令：**show switchport interface [ethernet <interface-list>]**
功能：显示交换机端口的 VLAN 端口模式和所属 VLAN 号及交换机的 Trunk 端口信息。
参数：***<interface-list>***为端口号，可以是 0/0/1-24,0/1/1,0/2/1
命令模式：特权用户配置模式
举例：显示端口 0/1 的 VLAN 信息。
Switch#show switchport interface ethernet 0/0/1
Ethernet0/0/1
State:Universal

Mac addr num:-1
Mode :Access
Access Vlan :1
Trunk native Vlan :1
Trunk allowed Vlan :ALL

显示内容	描述
Ethernet0/01	对应的以太网接口号；
State	当前接口的状态；
Mac addr num	当前接口具备学习MAC地址的数量；
Mode :Access	当前接口的VLAN模式；
Access Vlan :1	当前接口从属的VLAN号；
Trunk native Vlan :1	交换机Trunk本地VLAN的PVID；
Trunk allowed Vlan :ALL	Trunk允许通过的VLAN。

5.2.5.10 show tcp

命令：show tcp
功能：显示当前与交换机建立的 TCP 连接情况。
命令模式：特权用户配置模式
举例：
Switch#show tcp
LocalAddress LocalPort ForeignAddress ForeignPort State
0.0.0.0 23 0.0.0.0 0 LISTEN
0.0.0.0 80 0.0.0.0 0 LISTEN

显示内容	描述
LocalAddress	tcp连接的本地地址
LocalPort	tcp连接的本地段口号
ForeignAddress	tcp连接的对端的地址
ForeignPort	tcp连接的对端的端口号
State	tcp连接所处的当前的状态

5.2.5.11 show udp

命令：show udp
功能：显示当前与交换机建立的 UDP 连接情况。
命令模式：特权用户配置模式
举例：
SWITCH#show udp
LocalAddress LocalPort ForeignAddress ForeignPort State
0.0.0.0 161 0.0.0.0 0 CLOSED
0.0.0.0 123 0.0.0.0 0 CLOSED

0.0.0.0 1985 0.0.0.0
0 CLOSED

显示内容	描述
LocalAddress	udp连接的本地地址
LocalPort	udp连接的本地段口号
ForeignAddress	udp连接的对端的地址
ForeignPort	udp连接的对端的端口号
State	udp连接所处的当前的状态

5.2.5.12 show telnet login

命令：show telnet login
功能：显示当前与交换机建立器 Telnet 连接的 Telnet 客户端的信息。
使用指南：本命令用以查看当前登录到系统的远程用户的信息。
举例：
Switch#show telnet login
Authenticate login by local.
Login user:
aa

5.2.5.13 show telnet user

命令：show telnet user
功能：显示所有已授权可以通过 Telnet 访问交换机的 Telnet 客户端的信息。
使用指南：本命令用以查看当前系统已授权的所有 Telnet 客户端的信息。
举例：
Switch#show telnet user
Authenticate login by local.
Login user:
aa
相关命令：telnet-user password

5.2.5.14 show version

命令：show version
功能：显示交换机版本信息。
命令模式：特权用户配置模式
使用指南：通过查看版本信息可以获知硬件和软件所支持的功能特性。
举例：
Switch#show version
DCRS5526S Device, Nov 4 2003 21:30:14
HardWare version is 2.00, SoftWare version is 2.1, BootRom version is 1.1.4
Copyright (C) 2001-2002 by Digitalchina Networks Limited.

5.2.6debug

DCRS-5526S 支持的每一项协议都有相应的 debug 命令，用户可以通过查看 debug 命令的显示信息诊断网络故障。在以后的章节中会陆续介绍到相应协议的 debug 命令。

5.3 配置交换机的 IP 地址

DCRS-5526S 所有以太口接口都默认为二层端口 DataLink Layer，进行二层转发，如果希望将某一个端口设置为三层端口 Network Layer，并且为该端口设置 ip 地址，就需要使用 no switchport 命令将其转化为三层端口，这样才可以及在该设备之上实施三层相关命令。而接口 vlan(interface vlan)代表了某一个 vlan 的接口功能，vlan 相关的所有接口配置命令都可以在接口 vlan 的模式下配置。DCRS-5526S 为用户提供了三种配置 IP 地址的方式：

- 手工配置方式
- BootP 方式
- DHCP 方式

手工配置 IP 地址，即用户为交换机指定一个 IP 地址。

BootP/DHCP 方式是交换机作为 BootP/DHCP Client，向 BootP/DHCP Server 发出 BootPRequest（申请获取地址的请求包）广播包，BootP/DHCP Server 接收到请求后将地址分配给交换机。另外 DCRS-5526S 还具有了 DHCP Server 的功能，能够动态的为 DHCP Client 分配 IP 地址、网关地址及 DNS 服务器地址等网络参数。具体 DHCP Server 的配置参见后续章节。

5.3.1配置交换机的 IP 地址任务序列

1.手工配置方式
2.BootP 方式
3.DHCP 方式

1.手工配置方式

命令	解释
ip address <*ip_address*> <*mask*> **no ip address <*ip_address*> <*mask*>**	配置交换机的 IP 地址；本命令的 no 操作为删除交换机的 IP 地址。

2.BootP 方式

命令	解释
ip bootp-client enable **no ip bootp-client enable**	使能交换机为 BootP Client，通过 BootP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 BootP Client 功能。

3.DHCP

命令	解释
ip dhcp-client enable **no ip dhcp-client enable**	使能交换机为 DHCP Client，通过 DHCP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 DHCP Client 功能。

5.3.2配置交换机 IP 地址的命令

5.3.2.1 ip address

命令：ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

功能：设置交换机的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。

参数：<*ip-address*>为 IP 地址，点分十进制格式；**<*mask*>**为子网掩码，点分十进制格式；**[secondary]**为表示配置的 IP 地址为从 IP 地址。

缺省情况：出厂时交换机无 IP 地址。

命令模式：VLAN 接口配置模式

使用指南：用户若要为交换机配置 IP 地址，必须首先创建一个 VLAN 接口。

举例：设置 VLAN1 接口的 IP 地址为 10.1.128.1/24。

Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.1 255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#

相关命令：ip bootp-client enable、ip dhcp-client enable

5.3.2.2 ip bootp-client enable

命令：ip bootp-client enable

no ip bootp-client enable

功能：使能交换机为 BootP Client，通过 BootP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 BootP Client 功能，并且释放以 BootP 方式获取的地址和网关地址。

缺省情况：缺省关闭 BootP Client 功能。

命令模式：VLAN 接口配置模式

使用指南：通过 BootP 方式获取 IP 地址和手工配置、DHCP 方式获取 IP 地址是互斥的，不允许同时打开两种获取 IP 地址的方式。注意：要获得 IP 地址，网络上需要有 DHCP Server。

举例：通过 BootP 方式获取 IP 地址。

Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip bootp-client enable
Switch(Config-If-Vlan1)#no shutdown
Switch(Config-If-Vlan1)#exit
Switch(Config)#

相关命令：ip address、ip dhcp-client enable

5.3.2.3 ip dhcp-client enable

命令：ip dhcp-client enable
no ip dhcp-client enable
功能：使能交换机为 DHCP Client，通过 DHCP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 DHCP Client 功能，并且释放以 DHCP 方式获取的地址和网关地址。
缺省情况：缺省关闭 DHCP Client 功能。
命令模式：VLAN 接口配置模式
使用指南：通过 DHCP 方式获取 IP 地址和手工配置、BootP 方式获取 IP 地址是互斥的，不允许同时打开两种获取 IP 地址的方式。注意：要获得 IP 地址，网络上需要有 DHCP Server。
举例：通过 DHCP 方式获取 IP 地址。

```
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip dhcp-client enable
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#
```

相关命令：ip address、ip bootp-client enable

5.4 SNMP 配置

5.4.1SNMP 介绍

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前使用最广泛的网络管理协议，大量应用于以 TCP/IP 为基础的计算机网络。SNMP 是一个不断发展着的协议：SNMP v1 简单、易实现，被众多厂家支持； SNMPv2c 对 v1 的功能进行了部分修正和丰富，开始支持分层式的网管；SNMPv3 在安全性上做了极大的扩充，添加了 USM（基于用户的安全模型）和 VACM（基于视图的访问控制模型）子系统。

SNMP 协议提供了一个在网络中两点之间交换管理信息的直接的、基本的方法。SNMP 采用轮询的消息查询机制，采用被广泛使用的面向无连接的传输层协议 UDP 来传输消息，因此能够很好的被现有的计算机网络支持。

SNMP 协议采用管理站/代理模式，因此 SNMP 结构包括两个部分：NMS 网络管理站（Network Management Station），是运行支持 SNMP 协议的网管软件客户端程序的工作站，在 SNMP 的网络管理中起核心作用。Agent 代理，是运行在被管理网络设备上的服务器端软件，直接管理被管对象。NMS 利用通信手段，通过 Agent 代理来管理各被管对象。（本款及后续系列交换机都具有 Agent 代理功能）。

SNMP 的 NMS 和 Agent 之间通过标准消息进行通信，采取客户/服务器模式，由 NMS 发出请求，Agent 做出应答。SNMP 共有 7 种消息类型：

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request

- Set-Request
- Trap
- Inform-Request

NMS 通过 Get-Request、Get-Next-Request，Get-Bulk-Request 和 Set-Request 消息来对 Agent 发出查询和设置管理变量的请求，Agent 在收到请求后，用 Get-Response 消息来对请求进行回复。在某些特殊情况下，如网络设备端口 UP/DOWN、网络拓朴变化时候，Agent 会主动的向 NMS 发送 Trap 消息来通知 NMS 发生了异常事件。（当然，NMS 还可以通过设置 RMON 功能，自行对一些情况设置警报，当设定的警报事件触发后，Agent 将根据设置发送 Trap 或记录 Log，关于 RMON，下面有具体介绍）。Inform-Request 主要用于 NMS 之间进行通信，一般应用于分层式的网络管理。

USM 提供了完善的加密和鉴别服务，保证了传输的安全性。根据用户输入的密码，USM 对报文进行加密，保证报文在传输过程中不被察看，对报文进行鉴别，保证报文在传输过程中不被修改。USM 的标准加密算法为 DES-CBC 算法，鉴别算法为 HMAC-MD5 和 HMAC-SHA 算法。同时 USM 提供了时间窗的检查，防止网络延迟和重播的干扰。

VACM 提供了优秀的用户鉴权服务，保证了访问的安全性。VACM 将访问权限相同的用户放入同一组中，并为组划分了读写和通告操作的安全范围，有效地防止了用户的越权行为。

5.4.2MIB 介绍

NMS 可以访问的网管信息是经过精确的定义的，被完备的组织在一个管理信息数据库中，即 MIB。所谓 **MIB 管理信息库**（Management Information Base），是对于通过网络管理协议可以访问信息的精确定义。它使用一个层次化、结构化的形式，定义了可以从被监测网络设备上获得的管理信息。ISO ASN.1 为 MIB 定义了一个树型结构，每个 MIB 都用这种树型结构来组织所有的可用信息，树的每个节点都包含一个 OID 对象标识符(Object Identifier)和一个关于该节点的简短文本描述。OID 是有句点隔开的一组整数，它命名节点并且可以由它指示该节点在 MIB 树型结构中的位置，如下图所示：

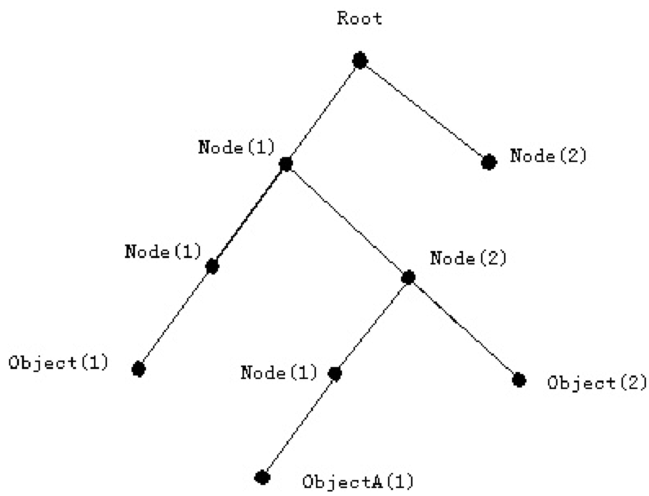


图 5-1 ASN.1 树实例

在该图中，对象 A 的 OID 为 1.2.1.1，NMS
通过这个独一无二的 OID，可以没有歧义的访问到这个对象，从而获取这个对象包含的标准变量。MIB 就按照这个结构定义了一个所监控网络设备的标准变量的集合。

如果您需要浏览 Agent 的 MIB 中的变量信息，需要在 NMS 上运行 MIB 浏览软件，如神州数码网络（北京）有限公司的网管软件 LinkManager 中的 MIB 浏览器等。Agent 上的 MIB 一般包括公有 MIB 和私有 MIB 两部分，公有 MIB 内定义的是公开的，所有 NMS 都可以访问的网络管理信息，私有 MIB 内定义的是各设备特有的属性信息，需要设备厂商的支持才可以浏览和控制。

MIB-I [RFC1156]是 SNMP 公有 MIB 库的第一个版本，后来经过扩充，被 MIB-II [RFC1213]所取代，MIB-II 保留了 MIB-I 在原来的 MIB 树中的对象标识符。MIB-II 下面包含很多子树，我们将之称为组，这些组里的对象覆盖了网络管理的各个功能域，NMS 通过访问 SNMP Agent 的 MIB 库，就可以得到相应的网络管理信息。

神州数码交换机可以做为 SNMP Agent，支持 SNMPv1/v2c 和 SNMPv3。神州数码交换机支持基本的 MIB-II、RMON 公有 MIB，还支持 BRIDGE MIB 等相关公有 MIB，同时支持自定义的私有 MIB，基本涵盖了本款交换机所涉及的各个相关参数，为网管软件管理提供全面的支持。

5.4.3RMON 介绍

RMON 是对 SNMP 标准基本体系的最重要的扩充。RMON 是一套 MIB 定义，其作用是定义标准的网络监视功能和接口，使基于 SNMP 的管理终端和远程监视器之间能够通信。RMON 提供了一种有效并且高效的方法来监视子网范围内的行为。

RMON 的 MIB 分为 10 组，该交换机支持其中最常用的 1、2、3、9 组，即：

统计组(statistics)：维护代理监视的每一个子网的基本使用和错误统计。

历史组(history)：记录从统计组可得到的信息的周期性统计样本。

警报组(alarm)：允许管理控制台人员为 RMON 代理记录的任何计数或整数设置采样间隔和报警阈值。

事件组(event)：一个关于由 RMON 代理产生的所有事件的表。

其中，警报组需要事件组的实现。统计组和历史组是显示现在或以前的一些子网统计数据。警报组和事件组则提供了一种可以监视网络上任意整数型数据变化的方法，并在数据异常时提供一些警告动作（发送 Trap 或者记录 Log）。

5.4.4SNMP 配置

5.4.4.1 SNMP 配置任务序列

1.打开或关闭 SNMP 代理服务器功能
2.配置 SNMP 团体字符串及代理设备的属性
3.配置 SNMP 管理站地址
4.配置引擎号
5.配置用户
6.配置组

7.配置视图
8.配置 TRAP
9.启动/关闭 RMON

1.打开或关闭 SNMP 代理服务器功能

命令	解释
snmp-server enable **no snmp-server enable**	打开交换机作为 SNMP 代理服务器功能；本命令的 no 操作为关闭 SNMP 代理服务器功能。

2.配置 SNMP 团体字符串

命令	解释
snmp-server community {ro|rw} <*string*> **no snmp-server community <*string*>**	设置交换机的团体字符串；本命令 no 操作为删除配置的团体字符串。

3.配置 SNMP 管理站地址

命令	解释
snmp-server securityip <*ip-address*> **no snmp-server securityip <*ip-address*>**	设置允许访问本交换机的 NMS 管理站的安全 IP 地址。
snmp-server SecurityIP enable **snmp-server SecurityIP disable**	打开/关闭 NMS 管理站的安全 IP 地址检查功能。

4.配置引擎号

命令	解释
snmp-server engineid < *engine-string* > **no snmp-server engineid < *engine-string* >**	设置交换机的本地引擎号，用于 v3。

5.配置用户

命令	解释
snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}] **no snmp-server user <*user-string*> <*group-string*>**	为一个 SNMP 的组添加一个新用户，完成 USM 配置，用于 v3。

6.配置组

命令	解释
snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv} [[read <*read-string*>] [write <*write-string*>] [notify <*notify-string*>]] **no snmp-server group <*group-string*>**	设置交换机的组信息，完成 VACM 配置，用于 v3。

{NoauthNopriv|AuthNopriv|AuthPriv}	

7.配置视图

命令	解释
snmp-server view <*view-string*> <*oid-string*> {include|exclude} **no snmp-server view <*view-string*>**	设置交换机的视图信息，用于 v3。

8.配置 **TRAP**

命令	解释
snmp-server enable traps **no snmp-server enable traps**	设置允许设备发送 Trap 消息，用于 v1/v2c/v3。
snmp-server host <*host-address* > {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*> **no snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv |AuthPriv}}} <*user-string*>**	设置接收 SNMP 的 Trap 消息的网络管理站 IP 地址，v1/v2c 中的 Trap 团体字符串，v3 中的用户名和安全级别。

9.启动**/**关闭 **RMON**

命令	解释
rmon enable **no rmon enable**	打开/关闭 RMON。

5.4.4.2 SNMP 配置命令

5.4.4.2.1 snmp-server enable

命令：snmp-server enable
no snmp-server enable

功能：打开交换机作为 SNMP 代理服务器功能；本命令的 no 操作为关闭 SNMP 代理服务器功能。

命令模式：全局配置模式

缺省情况：系统缺省关闭 SNMP 代理服务器功能。

使用指南：交换机若要通过网管软件进行配置管理，必须首先使用本命令打开交换机的 SNMP 代理服务器功能。

举例：打开交换机的 SNMP 代理服务器功能。

Switch(Config)#snmp-server enable

5.4.4.2.2 snmp-server community

命令：**snmp-server community {ro|rw} <*string*>**

no snmp-server community <*string*>

功能：设置交换机的团体字符串；本命令 no 操作为删除配置的团体字符串。

命令模式：全局配置模式

参数：**<*string*>**为设置的团体字符串；

ro|rw 为指定对 MIB 库的访问方式，**ro** 只读方式还是 **rw** 读写方式。

使用指南：交换机支持最多 4 个团体字符串。

举例：

添加读写权限的团体字符串 private。

Switch(config)#snmp-server community rw private

添加只读权限的团体字符串 public。

Switch(config)#snmp-server community ro public

修改原读写权限的团体字符串 private 为只读权限。

Switch(config)#snmp-server community ro private

删除团体字符串 private。

Switch(config)#no snmp-server community private

5.4.4.2.3 snmp-server enable traps

命令：**snmp-server enable traps**

no snmp-server enable traps

功能：设置允许设备发送 Trap 消息；本命令的 no 操作为禁止发送 Trap 消息。

命令模式：全局配置模式

缺省情况：系统缺省禁止发送 trap 消息。

使用指南：当设备允许发送 Trap 消息时，如果设备的端口发生 down/up 或者系统发生 down/up 等现象时，设备都会向接收 Trap 消息的管理站发送 Trap 消息。

举例：

允许发送 trap 消息

Switch(config)#snmp-server enable traps

禁止发送 trap 消息

Switch(config)#no snmp-server enable trap

5.4.4.2.4 snmp-server engineid

命令：**snmp-server engineid < *engine-string* >**

no snmp-server engineid < *engine-string* >

功能：配置引擎号；本命令的 no 操作为恢复默认引擎号。

命令模式：全局配置模式

参数：<engine-string>为引擎号，为 10 位十
六进制字符
缺省情况：缺省值为企业号+本机 MAC 地址。
使用指南：
举例：配置当前引擎号为 A66688999F
Switch(config)#snmp-server engineid A66688999F
恢复默认引擎号
Switch(config)#no snmp-server engineid A66688999F

5.4.4.2.5 snmp-server user

命令：snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}]
no snmp-server user <*user-string*> <*group-string*>

功能：为一个 SNMP 的组添加一个新用户；本命令的 no 操作为删除这个用户。
命令模式：全局配置模式
参数：<user-string>为用户名称，1-32 个字符；
<group-string>为用户所属的组名，1-32 个字符；
encrypted 对报文使用 DES 进行加密；
auth 对报文进行鉴别
md5 使用 HMAC MD5 算法鉴别
sha 使用 HMAC SHA 算法鉴别
<password-string>用户密码，1-32 个字符
使用指南：如果不选择是否加密鉴别，默认为不加密不鉴别。如果选择进行加密，则必须选择进行鉴别。删除一个用户时，如果输入正确的用户名和错误的组名，同样可以删除用户。
举例：
为组 DCNGroup 加入一个用户 tester，安全级别为需要加密、使用 HMAC md5 鉴别，密码 hello
Switch (Config)#snmp-server user tester DCNGroup encrypted auth md5 hello
删除一个用户
Switch (Config)#no snmp-server user tester DCNGroup

5.4.4.2.6 snmp-server group

命令：snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv} [[read <*read-string*>] [write <*write-string*>] [notify <*notify-string*>]]
no snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv}
功能：该命令用来配置一个新的组；本命令的 no 操作为删除这个组。
命令模式：全局配置模式
参数：<group-string > 组名，为 1-32 个字符；
NoauthNopriv 采用不鉴别不加密的安全级别
AuthNopriv 采用鉴别不加密的安全级别

AuthPriv 采用鉴别且加密的安全级别
read-string 可用于读的视图名，为 1-32 个字符
write-string 可用于写的视图名，为 1-32 个字符
notify-string 可用于通告（trap）的视图名，为 1-32 个字符

使用指南：系统含一个默认视图为 v1defaultviewname，建议采用这个视图作为通告的视图名。如果读或写视图为空，则禁止相应操作。

举例：

创建一个组 DCNGroup，安全级别为鉴别且加密，用于读的视图名为 readview,禁止写操作
Switch (Config)#snmp-server group DCNGroup AuthPriv read readview
删除组
Switch (Config)#no snmp-server group DCNGroup AuthPriv

5.4.4.2.7 snmp-server view

命令：snmp-server view <*view-string*> <*oid-string*> {include|exclude}
no snmp-server view <*view-string*>

功能：该命令用来创建或者更新视图的信息；本命令的 **no** 形式用来删除视图信息。

命令模式：全局配置模式

参数：< **view-string** > 视图名，为 1-32 个字符；
< oid-string > OID 号或者对应的节点名，为 1-255 个字符
include|exclude 包含/不包含此 OID

使用指南：该命令不仅支持以变量 OID 的字符串作为参数输入，同时还支持以节点名作为参数输入。

举例：

创建一个视图名为 readview，包含 iso 节点，但不包含 iso.3 节点
Switch (Config)#snmp-server view readview iso include
Switch (Config)#snmp-server view readview iso.3 exclude
删除视图
Switch (Config)#no snmp-server view readview

5.4.4.2.8 snmp-server host

命令：snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*>
no snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv |AuthPriv}}} <*user-string*>

功能：对 v1/v2c 版本来说，设置接收 SNMP 的 Trap 消息的网络管理站 IP 地址及 Trap 团体字符串，对 v3 版本来说，设置接收 SNMP 的 Trap 消息的网络管理站 IP 地址及 Trap 用户名和安全级别；本命令的 no 操作为取消这个 IP 地址。

命令模式：全局配置模式

参数：<***host-addr***>为接收 Trap 消息的 NMS 管理站 IP 地址；
v1|v2c|v3 发送 trap 使用的版本号
NoauthNopriv|AuthNopriv|AuthPriv 发送 v3 trap 使用的安全级别，不鉴别不加密|鉴别不加密|鉴别且加密

<user -*string*>v1/v2c 时为发送 Trap 消息时使用的 community 字符串，v3 时为用户名。

使用指南：本命令设置发送 Trap 的团体字符串是 RMON 事件组团体字符串的缺省值。如果 RMON 事件组没有设置团体字符串，则发送 RMON 的 Trap 时使用本命令设置的团体字符串；如果 RMON 事件组设置团体字符串，则发送 RMON 的 trap 时按照 RMON 设置的团体字符串发送。

举例：

设置一个接受 Trap 的 IP 地址。

Switch(config)#snmp-server host 1.1.1.5 v1 dcntrap

删除一个接受 Trap 的 IP 地址。

Switch(config)#no snmp-server host 1.1.1.5 v1 dcntrap

5.4.4.2.9 snmp-server securityip

命令：snmp-server securityip <*ip-address*>

no snmp-server securityip <*ip-address*>

功能：设置允许访问本交换机的 NMS 管理站的安全 IP 地址；本命令的 no 操作为删除配置的安全 IP 地址。

命令模式：全局配置模式

参数：<*ip-address*>为 NMS 的安全 IP 地址，点分十进制格式。

使用指南：只有 NMS 管理站的 IP 地址与本命令设置的安全 IP 地址相一致，它发出的 SNMP 包才会被交换机处理，该命令只适用于 SNMP v1 和 SNMP v2c。

举例：

设置 NMS 管理站的安全 IP 地址

Switch(config)#snmp-server securityip 1.1.1.5

删除安全 IP 地址

Switch(config)#no snmp-server securityip 1.1.1.5

5.4.4.2.10 snmp-server SecurityIP enable

命令：snmp-server SecurityIP enable

snmp-server SecurityIP disable

功能：打开/关闭 NMS 管理站的安全 IP 地址检查功能。

命令模式：全局配置模式

缺省情况：打开安全 IP 地址检查功能

举例：

关闭安全 IP 地址检查功能

Switch(config)#snmp-server securityip disable

5.4.4.2.11 rmon enable

命令：rmon enable

no rmon enable

功能：打开 RMON；本命令的 no 操作为关闭 RMON。
命令模式：全局配置模式
缺省情况：系统缺省关闭 RMON。
举例：
启动 RMON。
Switch(config)#rmon enable
关闭 RMON。
Switch(config)#no rmon enable

5.4.5SNMP 典型配置举例

管理站（NMS）的 IP 地址是 1.1.1.5；交换机（Agent）的 IP 地址是 1.1.1.9。
案例 1：管理站的网管软件使用 SNMP 协议从交换机获取数据。
配置步骤如下：
Switch(config)#snmp-server enable
Switch(Config)#snmp-server community rw private
Switch(Config)#snmp-server community ro public
Switch(Config)#snmp-server securityip 1.1.1.5

这样，管理站就可以使用 private 作为团体字符串对交换机进行可读写的访问，也可以使用 public 作为团体字符串对交换机进行只读的访问。

案例 2：管理站要接收来自交换机的 v1 Trap 消息（注：管理站可能设置了对 Trap 的团体字符串的验证，那么此例假设管理站的 Trap 验证团体字符串为 dcntrap）。
配置步骤如下：
Switch(config)#snmp-server enable
Switch(Config)#snmp-server host 1.1.1.5 v1 dcntrap
Switch(Config)#snmp-server enable traps

案例 3：管理站的网管软件使用 SNMP v3 协议从交换机获取数据。
配置步骤如下：
Switch(config)#snmp-server enable
Switch (Config)#snmp-server user tester DCNGroup encrypted auth md5 hello
Switch (Config)#snmp-server group DCNGroup AuthPriv read max write max notify max
Switch (Config)#snmp-server view max 1 include

案例 4：管理站要接收来自交换机的 v3Trap 消息
配置步骤如下：
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 10.1.1.2 v3 AuthPriv tester
Switch(config)#snmp-server enable traps

5.4.6SNMP 排错帮助

5.4.6.1监测和调试命令

5.4.6.1.1 show snmp

命令：**show snmp**
功能：显示 SNMP 各种计数器信息。
命令模式：特权配置模式
举例：

```
Switch#show snmp
0 SNMP packets input
        0 Bad SNMP version errors
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
0 SNMP packets output
        0 Too big errors (Max packet size 1500)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Get-response PDUs
        0 SNMP trap PDUs
```

显示内容	解释
snmp packets input	输入的 snmp 报文的总数
bad snmp version errors	版本信息错误的报文数目
unknown community name	团体名错误的报文数目
illegal operation for community name supplied	团体名对应的权限错误的报文数目
encoding errors	编码错误的 snmp 报文数目
Number of requested variables	nms 请求的变量的数目
number of altered variables	nms 设置的变量的数目
get-request PDUs	收到的 get 请求的报文数目
get-next PDUs	收到的 getnext 请求的报文数目
set-request PDUs	收到的 set 请求的报文数目
snmp packets output	输出的 snmp 报文的总数
too big errors	too_big 错误的 snmp 报文数目

maximum packet size	snmp 报文的最大长度
No such name errors	对不存在的 MIB 对象进行请求的报文的数目
bad values errors	bad_values 错误的 snmp 报文的数目
general errors	general_errors 错误的 snmp 报文的数目
response PDUs	发送的响应报文的数目
trap PDUs	发送的 trap 报文的数目

5.4.6.1.2 show snmp status

命令：**show snmp status**
功能：显示 SNMP 配置信息。
命令模式：特权用户配置模式
举例：
Switch#show snmp status
Trap enable
RMON enable
Community Information:
V1/V2c Trap Host Information:
V3 Trap Host Information:
Security IP Information:

显示内容	解释
Community string	团体字符串
Community access	团体字符串的读写方式
Trap-rec-address	接收 Trap 的 IP 地址
Trap enable	是否允许发送 trap 消息
SecurityIP	允许访问 Agent 的管理站 IP 地址

5.4.6.1.3 show snmp engineid

命令：**show snmp engineid**
功能：显示引擎号的命令。
命令模式：特权配置模式
举例：
Switch#show snmp engineid
SNMP engineID:3138633303f1276c Engine Boots is:1

显示内容	解释
SNMP engineID	引擎号

Engine Boots	引擎启动次数

5.4.6.1.4 show snmp user

命令：show snmp user
功能：显示用户信息的命令。
命令模式：特权配置模式
举例：
Switch#show snmp user
User name: initialsha
Engine ID: 1234567890
Auth Protocol:MD5   Priv Protocol:DES-CBC
Row status:active

显示内容	解释
User name	用户名
Engine ID	引擎号
Priv Protocol	使用的加密算法
Auth Protocol	使用的鉴别算法
Row status	用户状态

5.4.6.1.5 show snmp group

命令：show snmp group
功能：显示组信息的命令。
命令模式：特权配置模式
举例：
Switch#show snmp group
Group Name:initial   Security Level:noAuthnoPriv
Read View:one
Write View:<no writeview specified>
Notify View:one

显示内容	解释
Group Name	组名
Security level	安全级别
Read View	读视图名
Write View	写视图名
Notify View	通告视图名

<no writeview specified>	用户没有指定适用的视图名

5.4.6.1.6 show snmp view

命令：show snmp view
功能：显示视图信息的命令。
命令模式：特权配置模式
举例：
Switch#show snmp view
View Name:readview 1. -Included active
1.3. - Excluded active

显示内容	解释
View Name	视图名
1.和 1.3.	OID 号
Included	视图包含以此 OID 为根的子树
Excluded	视图不包含以此 OID 为根的子树
active	状态

5.4.6.1.7 show snmp mib

命令：show snmp mib
功能：显示本机支持的所有 MIB。
命令模式：特权配置模式

5.4.6.1.8 debug snmp packet

命令：debug snmp packet
no debug snmp packet
功能：打开 SNMP 的调试开关；本命令的 no 操作为关闭该调试开关。
命令模式：特权配置模式
使用指南： 当用户在使用 SNMP 时遇到问题，可以打开 SNMP 的调试开关，查找问题的原因。
举例：
Switch#debug snmp packet

5.4.6.2SNMP 排错帮助

在配置、使用 SNMP 时，可能会由于物理连接、配置错误等原因导致 SNMPS 未能正常运行。因此，用户应注意以下要点：

- ✧ 首先应该保证物理连接的正确无误；
- ✧ 其次，保证接口和链路协议是 UP（使用 show interface 命令），保证交换机和主机能互相 ping 通（使用 ping 命令）；
- ✧ 然后，务必确认交换机打开了 SNMP Agent 服务器功能（使用 snmp-server enable 命令）；
- ✧ 接着，保证为 NMS 配置安权 IP（使用 snmp-server securityip 命令）和团体字符串（使用 snmp-server community 命令）正确，因为只要有一个错误 SNMP 将不能正确和 NMS 通信；
- ✧ 如果需要使用 Trap 功能，务必打开 Trap 功能（使用 snmp-server enable traps 命令），为了保证 Trap 能发送到指定的主机，请记住正确配置 Trap 的目标主机的 IP 和团体字符串（使用 snmp-server host 命令）；
- ✧ 如果需要使用 RMON 功能，必须首先打开 RMON（使用 rmon enable 命令）；

在 SNMP 运行过程中，如果用户还有疑惑，可以使用 show snmp 命令查看 SNMP 收发包的统计信息；可以使用 show snmp status 命令查看 SNMP 的配置信息；可以使用 debug snmp packet 命令打开 SNMP 的调试开关，查看调试信息；

如果上述查看方式的尝试仍无法解决 SNMP 的问题，那么请与 DCN 技术服务中心联系。

5.5 交换机升级

DCRS-5526S 为用户提供了两种模式下的交换机升级：一、BootROM 模式；二、Shell 模式下的 TFTP 升级、FTP 升级。

5.5.1 BootROM 模式

在 BootROM 模式下升级交换机有两种升级方式：TFTP 和 FTP，可通过 BootROM 下的命令设置选择升级方式。

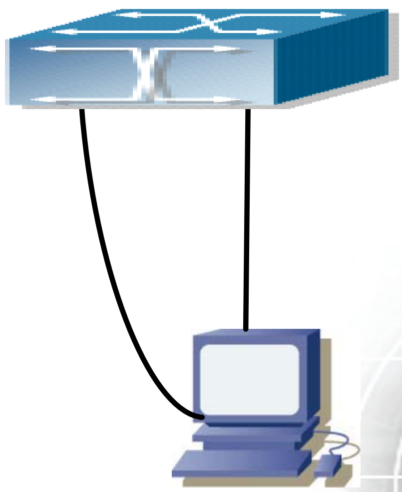


图 5-2 在 BootROM 模式下交换机升级的典型拓扑

升级步骤如下：

第一步：

如图将一台 PC 作为交换机的控制台，并且该控制台的以太网口与交换机的以太网口相连，在 PC 上安装有 FTP/TFTP 的服务器软件，及需要升级的 img 文件。

第二步：

在交换机启动的过程中，按住"ctrl＋b"键，直到交换机进入 BootROM 监控模式。操作显示如下：

DigitalChina Inc

Copyright (c) 2003 by DigitalChina Networks Ltd.
All rights reserved.

Testing RAM...
67,108,864 RAM OK.

Loading BootROM...
Starting BootRom...

AT49BV160

CPU: PowerPC MPC8245MH266, Revision 12
Version: 1.1.4
Creation date: Jul 17 2003, 14:01:12

Attached TCP/IP interface to sc0.

[Boot]:
[Boot]:
[Boot]:

第三步：

在 BootROM 模式下，执行命令 setconfig，设置本机在 BootROM 模式下的 IP 地址、掩码、服务器的 IP 地址、掩码及选择 TFTP 或者 FTP 的升级方式。如设置本机地址为 10.1.129.2/24，PC 地址为 10.1.129.66/24，选择 TFTP 升级方式，配置如下：

[Boot]: setconfig
Host IP Address: 10.1.1.1   192.168.1.189
Server IP Address: 10.1.1.2   192.168.1.101
FTP(1) or TFTP(2): 1   2
Network interface configure OK.
[Boot]:

第四步：
打开 PC 中 FTP/TFTP 服务器，如果是 TFTP 服务器，则运行 TFTP Server 程序；如果是 FTP 服务器，则运行 FTP Server 程序。在往交换机下传升级版本时，请先检查服务器与被升级交换机之间的连接状态，在服务器端使用 ping 命令，ping 通后，在交换机的 BootROM 模式下执行 load 命令；若 ping 不通，则检查原因。以下是更新系统映像文件的配置：

```
[Boot]: load nos.img
Loading...
entry = 0x10010
size = 0x1077f8
[Boot]: writeimg
Programming...

Program OK.
[Boot]:
```

第五步：
在 BootROM 模式下，执行命令 writeimg。以下是对更新系统映像文件的保存：
[Boot]: writeimg

第六步：
升级交换机成功，在 BootROM 模式下，执行命令 run，回到 CLI 配置界面。
[Boot]:run（或者 reboot）

5.5.2 FTP/TFTP 升级

5.5.2.1 FTP/TFTP 简介

FTP（File Transfer Protocol）/TFTP（Trivial File Transfer Protocol）都是文件传输协议，在TCP/IP协议族中处于第四层，即属于应用层协议，主要用于主机之间、主机与交换机之间传输文件。它们都采用客户机－服务器模式进行文件传输。下面是它们的不同之处。

FTP承载于TCP之上，提供可靠的面向连接数据流的传输服务，但它不提供文件存取授权，以及简单的认证机制（通过明文传输用户名和密码来实现认证）。FTP在进行文件传输时，客户机和服务器之间要建立两个连接：控制连接和数据连接。首先由FTP客户机发出传送请求，与服务器的21号端口建立控制连接，通过控制连接来协商数据连接。

数据连接有两种方式：

一种为主动连接。客户端是主动告诉服务器自己用于数据传输的地址和端口号，控制连接将一直保留到数据传输完成。接着服务器在20号端口没有被使用的条件下采用20号端口与客户机提供的地址和端口号建立数据连接，并传输数据；如果20号端口正在被使用，通过设置20号端口可以重用，服务器通过系统自动生成另外的端口号建立数据连接。

另外一种方式是被动连接。客户端通过控制连接告诉服务器端建立被动连接，服务器端就建立自己的数据监听端口，将这个端口通过控制连接告诉客户端，由客户端主动与指定地址的端口建立数据连接。

由于数据连接是通过指定的地址和端口号，还存在通过第三方来提供数据连接服务。

TFTP 承载在 UDP 之上，提供不可靠的数据流传输服务，同时也不提供用户认证机制以及根据用户权限提供对文件操作授权；它是通过发送包文，应答方式，加上超时重传方式来保证数据的正确传输。TFTP 相对于 FTP 的优点是提供简单的、开销不大的文件传输服务。

DCRS-5526S 实现 FTP/TFTP 客户机和服务器的功能。当 DCRS-5526S 作为 FTP/TFTP 客户机时，在不影响交换机正常工作的情况下，能从远端 FTP/TFTP 服务器（可以是主机和其它交换机）下载配置文件或系统文件，(FTP 客户端可以查看服务器上的文件列表)，也可以将 DCRS-5526S 当前配置文件或系统文件上载到远端 FTP/TFTP 服务器上（可以是主机和其它交换机）的功能；当 DCRS-5526S 作为 FTP/TFTP 服务器时，同样它能为它授权的 FTP/TFTP 客户机提供上传和下载文件的服务，（FTP 服务器还提供传输服务器上文件列表功能）。

下面介绍 FTP/TFTP 中经常用到的术语：

ROM：EPROM 的简称，可擦写只读寄存器。DCRS-5526S 采用 FLASH 内存条代替 EPROM。

SDRAM：交换机内存，用于系统软件的运行和配置序列的存放。

FLASH：闪存，用于保存系统文件和配置文件。

系统文件：包括系统映像文件和引导文件。

系统映像文件：是指交换机硬件驱动和软件支持程序等的压缩文件，即我们通常说的 IMG 升级文件。DCRS-5526S 系统映像文件只允许保存在 FLASH 中。DCRS-5526S 规定，在全局配置模式下通过 FTP 上载系统映像文件的文件名固定为 nos.img，拒绝其它系统 IMG 文件的上载。

引导文件：是指引导交换机初始化等的文件，即我们通常说的 ROM 升级文件（如果文件较大，可以压缩为 IMG 文件）。DCS 引导文件只允许保存在 ROM 中。DCRS-5526S 规定引导文件的文件名固定为 nos.rom。

配置文件：包括启动配置文件和运行配置文件。区分启动配置文件和运行配置文件便于实现配置的备份和更新。

启动配置文件：是指交换机启动时采用的配置序列。DCRS-5526S 启动配置文件只存放在 FLASH 中，即对应着所谓的配置保留。为了禁止非法文件的上载和方便配置，DCRS-5526S 规定，启动配置文件名固定为 startup-config。

运行配置文件：是指交换机当前运行的配置序列。DCRS-5526S 运行配置文件存放在内存中。目前，使用命令 **write** 或命令 **copy running-config startup-config**，可将运行配置序列 running-config 从内存中保存到 FLASH 中，即实现运行配置序列到启动配置文件的转变，形成配置保留。为了禁止非法文件的上载和方便配置，DCRS-5526S 规定，运行配置文件名固定为 running-config。

出厂配置文件：即 factory-config 文件，是 DCRS-5526S 出厂时的配置文件，使用命令 **set default** 和命令 **write**，重启后可将配置文件恢复成出厂配置文件。

5.5.2.2 FTP/TFTP 配置

DCRS-5526S 作为 FTP 或者 TFTP 客户机时，在配置上极其相似，因此本手册把 FTP 和 TFTP 作为客户机时的配置结合在一起说明。

5.5.2.2.1 FTP/TFTP 配置任务序列

1. TFTP 客户机配置
   （1）上载/下载配置文件或系统文件
2. FTP 客户机配置
   （1）载/下载配置文件或系统文件
   （2）查看服务器上文件列表
3. FTP 服务器配置
   （1）启动 FTP Server
   （2）配置 FTP 登录用户名和口令
   （3）修改 FTP Server 连接空闲时限
   （4）关闭 FTP Server
4. TFTP 服务器配置
   （1） 启动 TFTP Server
   （2） 配置 TFTP Server 连接空闲时限
   （3） 配置超时范围内没有收到应答报文的重传次数
   （4） 关闭 TFTP Server

1. FTP/TFTP 客户机配置

（1）FTP 客户机端上下载文件

命令	解释
特权用户配置模式	
copy <***source-url***> <***destination-url***> **[ascii | binary]**	FTP/TFTP 客户机上下载文件。
全局模式	
Dir <ftpServerUrl>	FTP 客户机查看服务器上文件列表 FtpServerUrl 为 ftp://user:password@IP Address 格式

2.FTP 服务器配置

（1）启动 FTP 服务器

命令	解释
全局配置模式	
ftp-server enable **no ftp-server enable**	启动 FTP Server；本命令的 no 操作为关闭 FTP Server 服务，禁止 FTP 用户登录。

（2）配置 FTP 登录用户名和口令

命令	解释
全局配置模式	
ip ftp-server username <*username*> password {0|7} <*password*> **no ip ftp-server username <*username*>**	配置 FTP 登录的用户名和口令；本命令的 no 操作为删除配置的用户名。

（3）修改 FTP Server 连接空闲时限

命令	解释
全局配置模式	
ftp-server timeout <seconds> **no ftp-server timeout**	设置连接空闲时限；本命令的 no 操作为恢复缺省值。

3.TFTP 服务器配置

（1）启动 TFTP 服务器

命令	解释
全局配置模式	
tftp-server enable **no tftp-server enable**	启动 TFTP Server；本命令的 no 操作为关闭 TFTP Server 服务，禁止 TFTP 用户登录。

（2）修改 TFTP Server 连接空闲时限

命令	解释
全局配置模式	
tftp-server transmission-timeout <seconds>	设置超时的时间间隔；

（3）修改 TFTP Server 连接重传次数

命令	解释
全局配置模式	
tftp-server retransmission-number < *number* >	设置超时时间内的最大重传次数。

5.5.2.2.2 FTP/TFTP 配置命令

5.5.2.2.2.1 copy（FTP）

命令：**copy** <***source-url***> **<*destination-url*> [ascii | binary]**

功能：FTP 客户机上下载文件。

参数：**<*source-url*>**为被拷贝的源文件或目录的位置；**<*destination-url*>**为文件或目录所要拷贝到的目的地址；**<*source-url*>**和**<*destination-url*>**的具体形式是随着文件或目录位置的不同而变化的。**ascii** 表示文件传输使用 ASCII 标准；**binary** 表示文件传输使用二进制标准（缺省传输方式）。当 URL 是 FTP 地址时的格式为：ftp://<*username*>:<*password*>@<*ipaddress*>/<*filename*>，其中<*username*>为 FTP 用户名，<*password*>为 FTP 用户口令，<*ipaddress*>为 FTP 服务器/客户机的 IP 地址，<*filename*>为 FTP 上下载文件名。

filename 的特殊关键字：

关键字	源地址或目的地址

running-config	运行配置文件
startup-config	启动配置文件
nos.img	系统文件
nos.rom	系统启动文件
stacking/nos.img	作为目的地址在堆叠模式下对 Slave 进行系统文件升级
stacking/nos.rom	作为目的地址在堆叠模式下对 Slave 进行系统启动文件升级

说明：该命令还支持在堆叠模式下的整体升级功能。注意这种整体升级的操作只能在 Master 上进行，并且只能对所有的 Slave 进行升级，Master 需另外升级。

命令模式：特权配置模式

使用指南：本命令支持命令行提示，即如果用户可以输入如下形式的命令 **copy <*filename*> ftp:**或者 **copy ftp: <*filename*>**后直接回车，系统会出现如下的提示：

ftp server ip address [x.x.x.x] >

ftp username>

ftp password>

ftp filename>

要求输入 FTP 服务器的地址、用户名、密码及文件名。

举例：

（1）储存 FLASH 内的映像到 FTP 服务器 10.1.1.1，FTP 服务器的登录用户名为 Switch，密码为 digitalchina：

Switch#copy nos.img ftp://Switch:digitalchina@10.1.1.1/nos.img

（2）从 FTP 服务器 10.1.1.1 上得到系统文件 nos.img，用户名为 Switch，密码为 digitalchina：

Switch#copy ftp://Switch:digitalchina@10.1.1.1/nos.img nos.img

（3）从 FTP 服务器 10.1.1.1 上得到系统文件 nos.img，用户名为 Switch，密码为 digitalchina，然后对堆叠模式下的 slave 交换机进行整体升级：

Switch#copy ftp://Switch:digitalchina@10.1.1.1/nos.img stacking/nos.img

（4）保存运行配置文件：

Switch#copy running-config startup-config

相关命令：write

5.5.2.2.2 dir <ftp-server-url>

命令：dir <ftp-server>

功能：查看 FTP 服务器上的文件列表

参数：< ftp-server-url **>** 格式为：ftp://<*username*>:<*password*>@<*ipaddress*>，其中<*username*>为 FTP 用户名，<*password*>为 FTP 用户口令，<*ipaddress*>为 FTP 服务器的 IP 地址。

命令模式：全局配置模式

5.5.2.2.3 ftp-server enable

命令：ftp-server enable

no ftp-server enable

功能：启动 FTP Server；本命令的 no 操作为关闭 FTP Server 服务，禁止 FTP 用户登录。
缺省情况：缺省不启动 FTP Server。
命令模式：全局配置模式
使用指南：当启动 FTP 服务器功能后，交换机仍保留 FTP 客户机的功能。系统缺省情况下不启动 FTP Server。
举例：打开 FTP Server 服务。
Switch#config
Switch(Config)# ftp-server enable
相关命令：**ip ftp-server username**

5.5.2.2.2.4 ftp-server timeout

命令：**ftp-server timeout <*seconds*>**
no ftp-server timeout
功能：设置数据连接空闲时限；本命令的 no 操作为恢复缺省值。
参数：**<*seconds*>**为 FTP 连接空闲时限，单位秒，取值范围为 5~4294967295。
缺省情况：系统缺省空闲时限为 600 秒。
命令模式：全局配置模式
使用指南：当 FTP 数据连接空闲实现超过此值时，切断 FTP 控制连接。
举例：修改空闲时限为 100 秒。
Switch#config
Switch(Config)#ftp-server timeout 100

5.5.2.2.2.5 ip ftp-server username

命令：**ip ftp-server username <*username*> password {0|7} <*password*>**
no ip ftp-server username <*username*>
功能：配置 FTP 登录的用户名和口令；本命令的 no 操作为删除配置的用户名。
参数：**<*username*>**为 FTP 连接的用户名，取值范围不超过 100 字符。**0|7** 分别表示明文显示和加密显示口令，**<*password*>**为 FTP 连接使用口令，取值范围不超过 127 字符。
缺省情况：系统缺省使用的口令为 username@Switchname.domain，其中变量 username 是当前用户名，Switchname 是交换机名，domain 是 Switch 的域名。
命令模式：全局配置模式
举例：配置用户名为 DCSwitch，密码为 digitalchina。
Switch#config
Switch(Config)# ip ftp-server username DCSwitch password 0 digitalchina

5.5.2.2.2.6 copy（TFTP）

命令：**copy** <***source-url*> <*destination-url*> [ascii | binary]**
功能：TFTP 客户机上下载文件。
参数：<***source-url*>**为被拷贝的源文件或目录的位置；**<*destination-url*>**为文件或目录所要拷贝到的目的地址；**<*source-url*>**和**<*destination-url*>**的具体形式是随着文件或目录位

置的不同而变化的。**ascii** 表示文件传输使用
ASCII 标准；**binary** 表示文件传输使用二进制标准（缺省传输方式）。当 URL 是 TFTP 地址时的格式为：tftp://<*ipaddress*>/<*filename*>，其中<*ipaddress*>为 TFTP 服务器/客户机的 IP 地址，<*filename*>为 TFTP 上下载文件名。
filename 的特殊关键字：

关键字	源地址或目的地址
running-config	运行配置文件
startup-config	启动配置文件
nos.img	系统文件
nos.rom	系统启动文件
stacking/nos.img	作为目的地址在堆叠模式下对 Slave 进行系统文件升级
stacking/nos.rom	作为目的地址在堆叠模式下对 Slave 进行系统启动文件升级

命令模式：特权用户配置模式
使用指南：本命令支持命令行提示，即如果用户可以输入如下形式的命令 **copy <*filename*> tftp:**或者 **copy tftp: <*filename*>**后直接回车，系统会出现如下的提示：
tftp server ip address>
tftp filename>
要求输入 TFTP 服务器的地址和文件名。
举例：
（1）储存 FLASH 内的映像到 TFTP 服务器 10.1.1.1
Switch#copy nos.img tftp:// 10.1.1.1/ nos.img

（2）从 TFTP 服务器 10.1.1.1 上得到系统文件 nos.img：
Switch#copy tftp://10.1.1.1/nos.img nos.img

（3）保存运行配置文件：
Switch#copy running-config startup-config
相关命令：write

5.5.2.2.2.7 tftp-server enable

命令：tftp-server enable
no tftp-server enable
功能：启动 TFTP Server；本命令的 no 操作为关闭 TFTP Server 服务，禁止 TFTP 用户登录。
缺省情况：缺省不启动 TFTP Server。
命令模式：全局配置模式
使用指南：当启动 TFTP 服务器功能后，交换机仍保留 TFTP 客户机的功能。系统缺省情况下不启动 TFTP Server。
举例：打开 TFTP Server 服务。
Switch#config
Switch(Config)#tftp-server enable
相关命令：tftp-server timeout

5.5.2.2.2.8 tftp-server retransmission-number

命令：tftp-server retransmission-number <*number*>
功能：设置 tftp 服务器重新传输数据的次数。
参数：**<*number*>**为重传次数，取值范围为 1~20。
缺省情况：系统缺省重传 5 次。
命令模式：全局配置模式
举例：修改重传次数为 10 次。
Switch#config
Switch(Config)#tftp-server retransmission-number 10

5.5.2.2.2.9 tftp-server transmission-timeout

命令：tftp-server transmission-timeout <*seconds*>
功能：设置 tftp 服务器传输超时时间。
参数：**<*seconds*>**为超时时间，取值范围为 5~3600s。
缺省情况：系统缺省超时时间为 600s。
命令模式：全局配置模式
举例：修改超时时间为 60s。
Switch#config
Switch(Config)#tftp-server transmission-timeout 60

5.5.2.3 FTP/TFTP 配置举例

案例 1：作为 FTP/TFTP 客户机
同步情况：交换机通过以太口和 PC 相连，PC 为 FTP/TFTP 服务器，IP 地址为 10.1.1.1，交换机作为 FTP/TFTP 客户端，交换机 VLAN1 接口 IP 地址为 10.1.1.2。从 PC 端下载交换机的 nos.img 文件。如图所示：

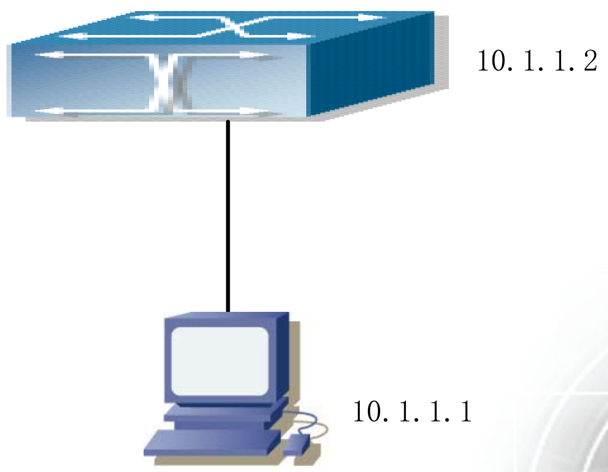


图 5-3 作为 FTP/TFTP client 下载 nos.img 文件

FTP 配置：
PC 端：

在 PC 机上启动 FTP Server 软件，并且设置
用户 Switch，密码为 digitalchina。并将 nos.img 放到 PC 的 FTP Server 的目录下。
DCRS-5526S：
Switch(Config)#inter vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#exit
Switch#copy ftp://Switch:digitalchina@10.1.1.1/nos.img nos.img
Switch#reload
这样交换机就将 PC 上的 nos.img 软件下载到 flash 了。
TFTP 配置：
PC 端：
在 PC 机上启动 TFTP Server 软件，并将 nos.img 放到 PC 的 TFTP Server 的目录下。
DCRS-5526S：
Switch(Config)#inter vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#exit
Switch#copy tftp://10.1.1.1/nos.img nos.img
Switch#reload

案例 2：DCRS-5526S 作为 FTP 服务器
DCRS-5526S 作为 FTP Server，PC 作为 FTP client，将交换机上的 nos.img 传送到 PC 机上。这里，交换机通过以太口和 PC 相连。

配置步骤如下：
Switch(Config)#inter vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#ftp-server enable
Switch(Config)#ip ftp-server username Switch password 0 digitalchina
PC 端：
通过 FTP Client 软件，登录到交换机，输入用户名 Switch，密码 digitalchina，通过 get nos.img nos.img 即可将交换机上的 nos.img 下载到 PC 上。

案例 3：作为 TFTP 服务器
DCRS-5526S 作为 TFTP Server，PC 作为 TFTP Client，将交换机上的 nos.img 传送到 PC 机上。这里，交换机通过以太口同 PC 相连，如图 4-4。

配置步骤如下：
Switch(Config)#inter vlan 1

Switch(Config-If-Vlan1)#ip address 10.1.1.2
255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#tftp-server enable
PC 端：
通过 TFTP Client 软件，登录到交换机，通过 tftp 命令即可将交换机上的 nos.img 下载到 PC 上。

案例 4：交换机作为 FTP 服务器提供客户机查看文件列表
交换机作为 FTP Server，PC 作为 FTP client，将交换机上的文件列表传送到 PC 机上。这里，交换机通过以太口和 PC 相连。

配置步骤如下：
Switch(Config)#inter vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#ftp-server enable
Switch(Config)# ip ftp-server username Switch password 0 digitalchina
PC 端：
通过 FTP Client 软件，登录到 DCRS-5526S，输入用户名 Switch，密码 digitalchina，通过 ls 命令或是 dir 命令
C:\>ftp 10.1.1.2
Connected to 10.1.1.2.
220 welcome your using ftp server...
User (10.1.1.2:(none)): Switch
331 User name okay,need password
Password:
230 User logged in,proceed
ftp> dir
200 PORT Command successful
150 ascii type in transfer file
file name file length
nos.img 1195841
nos.rom 557980
startup-config 2611
running-config
226 transfer complete.
ftp: 137 bytes received in 0.08Seconds 1.73Kbytes/sec.
ftp>ls
200 PORT Command successful
150 ascii type in transfer file
file name file length

nos.img 1195841
nos.rom 557980
startup-config 2611
running-config
226 transfer complete.
ftp: 137 bytes received in 0.08Seconds 1.73Kbytes/sec
ftp>

案例 5：交换机作为 FTP 客户机查看 FTP 服务器上文件列表
同步情况：交换机通过以太口和 PC 相连，PC 为 FTP 服务器，IP 地址为 10.1.1.1，交换机作为 FTP 客户端，交换机 VLAN1 接口 IP 地址为 10.1.1.2。查看 PC 机上 FTP 服务器上文件列表。

FTP 配置：
PC 端：
在 PC 机上启动 FTP Server 软件，并且设置用户 Switch，密码为 digitalchina。
交换机端设置：
Switch(Config)#inter vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#no shut
Switch(Config-If-Vlan1)#exit
Switch(Config)#dir ftp://Switch:digitalchina@10.1.1.1
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
recv total = 480
nos.img
nos.rom
parsecommandline.cpp
position.doc
qmdict.zip
shell 维护统计.xls
…(省略部分显示)
show.txt
snmp.TXT
226 Transfer complete.
Switch(Config)#

5.5.2.4 FTP/TFTP 排错帮助

5.5.2.4.1 监测和调试命令

5.5.2.4.1.1 show ftp

命令：show ftp
功能：显示 FTP 服务器参数的设置情况。
命令模式：特权用户配置模式
缺省情况：缺省不显示。
举例：
Switch#sh ftp↵
timeout :600

显示信息	描述
timeout	超时时间

5.5.2.4.1.2 show tftp

命令：show tftp
功能：显示 TFTP 服务器参数的设置情况。
缺省情况：缺省不显示。
命令模式：特权用户配置模式
举例：
Switch#sh tftp

timeout :60
Retry Times :10

显示信息	解释
Timeout	超时时间
Retry Times	重传次数

5.5.2.4.2 FTP 排错帮助

在使用 FTP 协议上下载系统文件时，务必保证链路的可达，即在使用 FTP 之前，使用 Ping 命令检验 FTP 客户机和服务器的是否可达。如 Ping 不通，则需查看相应排错信息，恢复链路的可达性。

☞ 下面是发送文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命令。

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
nos.img file length = 1526021
read file ok

send file
150 Opening ASCII mode data connection for nos.img.
226 Transfer complete.
close ftp client.

☞ 下面是接收文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命令。

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
recv total = 1526037
****
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.

☞ 如果交换机通过 FTP 升级系统文件或系统启动文件时，必须等待系统提示出现表示升级成功的"close ftp client."或"226 Transfer complete."的字样，此时交换机可以进行重启的操作，否则将回导致交换机的无法启动。若出现通过 FTP 升级系统文件及系统启动文件失败时，请重新升级或进入到 BootROM 模式升级。

5.5.2.4.3 TFTP 排错帮助

在使用 TFTP 协议上下载系统文件时，务必保证链路的可达，即在使用 TFTP 之前，使用 Ping 命令检验 TFTP 客户机和服务器的是否可达。如 Ping 不通，则需查看相应排错信息，恢复链路的可达性。

☞ 下面是发送文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命令。

nos.img file length = 1526021
read file ok
begin to send file,wait...
file transfers complete.
close tftp client.

☞ 下面是接收文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命令。

begin to receive file,wait...
recv 1526037
****
write ok
transfer complete
close tftp client.

如果交换机通过 TFTP 升级系统文件或系统启动文件时，必须等待系统提示出现表示升级成功的"close tftp client."的字样，此时交换机可以进行重启的操作，否则将回导致交换机的无法启动。若出现通过 TFTP 升级系统文件及系统启动文件失败时，请重新升级或进入到 BootROM 模式升级。

5.6 系统日志

5.6.1系统日志介绍

系统日志接管大多数的信息输出，并且能够进行细致的分类，从而能够有效地进行信息筛选，它通过与 Debug 程序的结合，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

神州数码交换机的系统日志具有以下一些特性：

- 支持控制台（Console）、Telnet终端和哑终端（monitor）、日志缓冲区（logbuf）、日志主机（loghost）、系统闪存(flash)五个方向的日志输出。
- 日志信息按重要性划分为四个等级，可按等级进行信息过滤。
- 日志信息按来源模块进行划分，可按模块进行信息过滤。

5.6.1.1日志输出通道

目前，神州数码交换机的系统日志，可以从五个方向（也称为日志通道）输出各种日志信息：

- 通过Console口向本地控制台输出日志信息。
- 向远程Telnet终端或哑终端输出日志信息，此功能有助于远程维护。
- 在交换机内部分配适当大小的日志缓冲区，用于记录日志信息。
- 配置日志主机，日志系统直接将日志信息发往日志主机，并在其上以文件的形式保存起来，供随时查看。
- 在交换机内部分配适当大小的flash缓冲区，和logBuf通道不同的是，此缓冲区的信息将在系统因任务异常重启时写入flash中，以便之后查错用。（建议此方向的日志信息要设置得精简一些）

每个输出方向通过配置命令指定所需要的通道，所有信息经过指定通道的过滤，发送到相应的输出方向；可根据需要配置输出方向所使用的通道，以及配置通道的过滤信息，完成各类信息的过滤以及重定向。

注意：五个方向的设置相互独立，但首先需要开启全局日志开关，设置才会生效。

5.6.1.2日志消息的严重等级（severity）

系统日志格式与 4.3 BSD UNIX 兼容，以便能够利用 UNIX/LINUX 上的 syslogd（系统日志守护进程），以及在 PC 机上运行的类似 syslogd 的一些应用程序来记录并分析日志。

在按严重等级来进行日志信息过滤时，采用的规则是：禁止严重等级大于所设置阈值的信息输出。越紧急的日志报文，其严重等级越小，critical 表示的等级为 2，debugging 为 7，因此，当设置严重等级阈值为 debugging 时，所有的信息都会输出。

严重等级 (Severity)	级别	描述	Syslog 定义
critical	2	Critical conditions 关键错误	LOG_CRIT

warnings	4	Warning conditions 警告，可能存在某种差错	LOG_WARNING
notifications	5	Normal but significant condition 需注意的信息	LOG_NOTICE
debugging	7	Debugging messages 调试信息	LOG_DEBUG

上述四类消息在以下情况下生成：

- 接口的up/down切换、拓扑变化、汇聚口状态变化等，显示级别为Warning。
- shell配置命令监控的输出，显示级别为notifications。

注意：系统日志缺省情况下处于关闭状态。在系统日志开启时，由于信息分类、输出的原因，特别是在处理信息较多时，对系统性能有一定的影响。

5.6.1.3日志消息的三级开关

整个系统日志按照全局日志开关、日志输出通道状态和通道过滤项的模块状态三级开关体系来控制日志消息的输出。

- 只有当全局日志开关为开，日志消息才被写入日志消息队列中。
- 交换机系统启动后，将启动系统日志任务。该任务的目的是不断从日志消息队列中取出每一条日志消息，然后将消息通过每一个输出通道输出。只有当输出通道状态为Enable时，日志消息才能够从该输出通道输出。
- 当日志消息进入输出通道后，利用输出通道的过滤项进行检查。只有日志消息的来源模块在过滤项中的状态为On时，日志消息才能够真正地从输出通道输出。

5.6.2系统日志配置

5.6.2.1系统日志配置任务序列

1. 设置全局日志开关
2. 设置控制台输出通道
3. 设置用户终端输出通道
4. 设置日志缓冲区输出通道
5. 设置日志主机输出通道
6. 设置 flash 输出通道
7. 显示日志通道信息
8. 设置日志输出通道过滤项

1.　设置全局日志开关

命令	描述
特权配置模式	
logging on **no logging on**	启动全局系统日志功能；在此命令前加"**no**"将关闭全局系统日志功能。

2.　设置控制台输出通道

命令	描述
特权配置模式	
logging console **no logging console**	打开控制台输出通道;在此命令前加"**no**"将关闭控制台输出通道的输出。

3.　设置用户终端输出通道

命令	描述
特权配置模式	
logging monitor **no logging monitor**	打开用户终端输出通道；在此命令前加"**no**"将关闭用户终端输出通道的输出。

4.　设置日志缓冲区输出通道

命令	描述
特权配置模式	
logging buffered [<*Maximum message count*>] **no logging buffered**	打开日志缓冲区输出通道；在此命令前加"**no**"将关闭日志缓冲区输出通道的输出。
show logging buffered [<*Maximum message count*>]	显示日志缓冲区通道的详细信息。
clear logging	清除日志缓冲区中的信息。

5.　设置日志主机输出通道

命令	描述
特权配置模式	
logging <*ip-addr*> [facility <*local-number*>] **no logging <*ip-addr*>**	打开日志主机输出通道；在此命令前加"**no**"将关闭日志主机输出通道的输出。

6.　设置flash输出通道

命令	描述
特权配置模式	
logging flash [<*Maximum message count* >] **no logging flash**	打开日志 flash 区输出通道；在此命令前加"**no**"将关闭日志 flash 区输出通道的输出。
show logging flash [<*Maximum message count* >]	显示日志 flash 区通道的详细信息。
clear logflash	清除日志 flash 区中的信息。
show logging lastfailureinfo	显示最近一次系统异常重起时记录在 flash 中的堆栈及 log 信息。

7.　显示日志通道信息

命令	描述

特权配置模式	
show channel [console | monitor | logbuff | loghost | flash]	显示日志通道的概要信息。

8. 设置日志输出通道过滤项

命令	描述
特权配置模式	
logging source {default|m_shell|sys_event} channel { console | flash | logbuff | loghost | monitor } [level { critical | debugging | notifications | warnings } [state { on | off }]] **no logging source { default | m_shell | sys_event } channel { console | flash | logbuff | loghost | monitor }**	向日志输出通道中添加过滤项记录。 从日志输出通道中删除过滤项记录。

5.6.2.2系统日志配置命令

5.6.2.2.1 clear logging

命令：**clear logging**
功能：该命令用来清除日志缓冲区中的信息。
命令模式：特权配置模式。
使用指南：用户需要清除日志缓冲区内的信息时，可使用本命令。
举例：清除日志缓冲区中的信息。
switch# clear logging ↵
相关命令：**show logging buffered**

5.6.2.2.2 clear logflash

命令：**clear logflash**
功能：该命令用来清除日志 flash 区中的信息。
命令模式：特权配置模式。
使用指南：用户需要清除日志 flash 区内的信息时，可使用本命令。
举例：清除日志缓冲区中的信息。
switch# clear logflash ↵
相关命令：**show logging flash**

5.6.2.2.3 logging buffered

命令：logging buffered [<*Maximum message count*>]

no logging buffered

功能：该命令用来打开日志缓冲区输出通道；在此命令前加“**no**”将关闭日志缓冲区输出通道的输出。

参数：***<Maximum message count>***为内存缓冲区的大小（指可容纳消息的条数），范围为10-1000。

命令模式：特权配置模式。

缺省情况：缺省为不向内存缓冲区输出日志信息。缺省设置的内存缓冲区大小为 100。

使用指南：只有启动了全局系统日志功能，该命令才会生效。

举例：使以太网交换机向内存缓冲区发送日志信息，设定内存缓冲区的大小为 50。

Switch# logging buffered 50↵

相关命令：**logging on**，**show channel logbuff**，**show logging buffered**

5.6.2.2.4 logging console

命令：logging console

no logging console

功能：该命令用于打开向控制台输出日志信息的通道；在此命令前加“**no**”将会关闭控制台输出通道的日志信息输出。

命令模式：特权配置模式。

缺省情况：缺省为不向控制台输出日志信息。

使用指南：只有启动了全局系统日志功能，该命令才会生效。

举例：打开向控制台输出日志信息的通道。

Switch#logging console↵

相关命令：**logging on**，**show channel console**

5.6.2.2.5 logging host

命令：logging <*ip-addr*> [facility <*local-number*>]

no logging <*ip-addr*>

功能：该命令用来打开日志主机输出通道；在此命令前加“**no**”将关闭日志主机输出通道的输出。

参数：***<ip-addr>***为日志主机的 IP 地址。

<local-number>为日志主机的记录工具，范围在 local0～local7。

命令模式：特权配置模式。

缺省情况：缺省为不向日志主机输出日志信息。缺省的日志主机的记录工具为 local0。

使用指南：只有启动了全局系统日志功能，该命令才会生效。

举例：使以太网交换机向 IP 地址为 100.100.100.5 的 PC 机发送日志信息，消息被保存到日志记录工具 local1 中。

Switch# logging 100.100.100.5 facility local1↵

相关命令：**logging on**，**show channel loghost**

5.6.2.2.6 logging monitor

命令：logging monitor

　　　no logging monitor

功能：该命令用来打开用户终端输出通道；在此命令前加“**no**”将关闭用户终端输出通道的输出。

命令模式：特权配置模式。

缺省情况：缺省为不向用户终端输出日志信息。

使用指南：只有启动了全局系统日志功能，该命令才会生效。

举例：打开向用户终端输出日志信息的通道。

Switch# logging monitor↵

相关命令：logging on，show channel monitor

5.6.2.2.7 logging on

命令：logging on

　　　no logging on

功能：该命令用来启动全局系统日志功能；在此命令前加“**no**”将关闭全局系统日志功能。

命令模式：特权配置模式。

缺省情况：缺省为不启动全局系统日志功能。

使用指南：只有启动了全局系统日志功能，系统才会向日志主机、控制台等方向输出系统日志信息。

举例：启动系统日志功能。

Switch# logging on↵

相关命令：logging host，logging buffered，logging console，logging monitor，logging flash ,show logging buffered

5.6.2.2.8 logging flash

命令：logging flash [<*Maximum message count*>]

　　　no logging flash

功能：该命令用来打开日志 Flash 输出通道；在此命令前加“**no**”将关闭日志 Flash 输出通道的输出。

参数：*<Maximum message count>*为 flash 缓冲区的大小（指可容纳消息的条数），范围为 10-1000。

命令模式：特权配置模式。

缺省情况：缺省为不向 flash 缓冲区输出日志信息。缺省设置的 flash 缓冲区大小为 100。

使用指南：只有启动了全局系统日志功能，该命令才会生效。保存在 flash 缓冲区的日志信息只在系统异常时才保存在硬件 flash 中

举例：使以太网交换机向 flash 缓冲区发送日志信息，设定 flash 缓冲区的大小为 50。

Switch# logging flash 50↵

相关命令：logging on，logging console，logging monitor，logging host， logging buffered，logging source

5.6.2.2.9 logging source

命令：**logging source {default| m_shell|sys_event} channel { console| flash | logbuff | loghost | monitor } [level { critical | debugging | notifications | warnings } [state { on | off }]]**

no logging source { default | m_shell | sys_event } channel { console | flash | logbuff | loghost | monitor }

功能：该命令用来向日志输出通道中添加/删除过滤项记录。

参数：**m_shell** 为允许 shell 模块输出日志消息。

sys_event 为允许系统重要事件输出日志消息（包括端口 UP/Down，拓朴变化等）

default 为允许所有模块输出日志消息。

channel { console| flash | logbuff | loghost | monitor }为要设置的输出通道名，即 console（控制台）, monitor（用户终端）, logbuff（日志缓冲区）,loghost（日志主机）与 flash（flash 区）。

level { critical | debugging | notifications | warnings }为日志消息的严重等级阈值，在此级别以下的信息不输出。

日志消息的严重级别信息如下：

critical - 严重信息
debugging - 调试过程产生的信息
notifications - 正常出现但是重要的信息
warnings - 警告信息

state { on | off }：该过滤项的状态为打开/关闭。

命令模式：特权配置模式。

缺省情况：缺省为向日志输出通道中添加过滤项记录，严重等级阈值缺省为 debugging。

使用指南：该命令可以配置日志输出通道针对模块级的过滤信息，例如实现 Driver 模块的日志信息输出到任何一个输出方向的过滤，Driver 模块的日志信息高于 warnings 级别的可以输出到日志主机，而高于 informational 可以输出到日志缓冲区，同时可以设置 Driver 模块的告警信息发送到特定的告警主机方向等功能，只需要在上述对应的通道进行过滤设置，则可以完成。而且可以通过相应的 no 命令从日志输出通道删除某一个过滤项。

注意：目前 source 只有两个模块可选：

一个为 m_shell，即监控所有配置命令，log 等级均为 notifications。

一个为 sys_event，即监控所有系统事件，包括端口 UP/Down，stp 拓扑变化，汇聚口汇聚状态变化等，log 等级均为 warnings。

举例：设置将 loghost 通道中的 shell 模块的日志类信息打开，且允许输出信息的最高级别为 notifications。设置将 logbuff 通道中的 shell 模块的日志类信息打开，且允许输出信息的最高级别为 debugging。

Switch# logging source m_shell channel loghost level notifications state on ↵
Switch# logging source m_shell channel logbuff level debugging state on ↵

相关命令：**logging on**，**logging console**，**logging monitor**，**logging host**， **logging buffered**，**logging flash**

5.6.3系统日志配置举例

神州数码交换机的管理 VLAN 的 IP 地址为 100.100.100.1，远端日志主机的 IP 地址为 100.100.100.5。需要能够将模块 shell 和系统事件的所有日志信息输出到远端日志主机的 local1 中，将模块 shell 严重等级为 warning 及 critical 的日志信息输出到日志缓冲区中。

配置步骤如下：

Switch#logging on

Switch#logging 100.100.100.5 facility local1

Switch#logging source m_shell channel loghost level debugging state on

Switch#logging source sys_event channel loghost level debugging state on

Switch#logging logbuffed 1000

Switch#logging source m_shell channel logbuff level warning state on

5.6.4系统日志排错帮助

5.6.4.1监测和调试命令

5.6.4.1.1 show channel

命令：show channel [console | monitor | logbuff | loghost | flash]

功能：该命令用来显示日志通道的概要信息。

参数： console 日志输出通道为控制台；monitor 日志输出通道为用户终端；logbuff 日志输出通道为日志缓冲区；loghost 日志输出通道为日志主机。flash 日志输出通道为系统闪存

命令模式：特权配置模式。

缺省情况：show channel 不带参数表示显示所有通道的概要信息。

使用指南：查看某日志通道的概要信息时，可使用本命令。

举例：显示 Loghost 通道的内容。

Switch# show channel loghost

/********* Loghost Channel ***************/

Channel ID:2, channel name:loghost

State: On

Send messages:0,Dropped messages:0

Loghosts:

IPAddress   Facility

100.100.100.5   local1

Filter Items:

Module   State   Servirity

shell   On   debugging

相关命令：logging on

5.6.4.1.2 show logging buffered

命令：**show logging buffered [<*Maximum message count*>]**

功能：该命令用来显示日志缓冲区通道的详细信息。

参数：**<*Maximum message count*>**为显示的日志消息条数。

命令模式：特权配置模式。

缺省情况：不带参数表示显示 100 条日志消息。

使用指南：如果当前日志缓冲区内的信息数少于用户指定的**<*Maximum message count*>**，则显示实际条数的日志信息。

举例：显示日志缓冲区通道中最新 20 条日志消息的详细信息。

```
Switch# show logging buffered 20↵
/********* Logbuff Channel ***************/
Channel ID:3, channel name:logbuff
State: On
Allowed max messages:100,Dropped messages:0,Current messages:0

Filter Items:
Module     State     Servirity
Driver     On        debugging

Msgs:
1. IFNET-5-UPDOWN:Line protocol on interface GigabitEthernet1/1, changed state to UP
2. EXEC-5-LOGIN: Console login from Console0
```

相关命令：**logging on，show channel logbuff**

5.6.4.1.3 show logging flash

命令：**show logging flash [<*Maximum message count*>]**

功能：该命令用来显示日志 flash 区通道的详细信息。

参数：**< *Maximum message count* >**为显示的日志消息条数。

命令模式：特权配置模式。

缺省情况：不带参数表示显示 100 条日志消息。

使用指南：如果当前日志缓冲区内的信息数少于用户指定的**<*Maximum message count*>**，则显示实际条数的日志信息。

举例：显示日志缓冲区通道中最新 20 条日志消息的详细信息。

```
Switch# show logging flash 20↵
/********* LogFlashChannel ***************/
Channel ID:4, channel name:logflash
State: On
Allowed max messages:100,Dropped messages:1,Current messages:1

Filter Items:
Module      State     Servirity
Shell       On        debugging
1 MON JAN 01 05:50:26 2001 <notifications> Shell[shellTask]:Exec command:logging
```

source m_shell channel flash
相关命令：**logging on，show channel flash**

5.6.4.1.4 show logging lastFailureInfo

命令：show logging lastFailureInfo
功能：该命令用来显示最近一次系统因任务异常而重起时的堆栈信息及当时的 flash 通道信息。
命令模式：特权配置模式。
举例：
Switch# show logging lastFailureInfo ↵
*********Last Failure Info**********
Last Fatal Error occured at MON JAN 01 00:16:14 2001
in <KillMe>
ERROR: Stack trace follows
FUNC = 0xf0e04, PC = 0xf0e70 (logMsg_ShowLoggingBuffered + 0x6c), SP = 0x1523db8
RA 0x0 out of range
ERROR: End of stack trace
*********Last log Info**********
1 MON JAN 01 05:50:26 2001 <notifications> Shell[shellTask]:Exec command:logging
source m_shell channel flash
相关命令：**logging on，show channel flash**

5.6.4.2系统日志排错帮助

当在使用系统日志功能出现问题时，请检查是否是如下原因：
- 检查全局系统日志开关是否打开；

5.7 配置分级

5.7.1配置分级介绍

为了对网络进行有效的保护，允许用户以不同的身份登录交换机进行配置，允许对不同的身份设置不同的密码，不同的身份在配置交换机时有不同的权限。目前DCN的交换机可以设置visitor和admin两种身份。两种登录身份的配置权限有以下区别：

登录身份	配置权限
visitor	绝大部分show命令以及ping、traceroute、clear等命令。该身份无法进入config模式
admin	所有命令

5.7.2配置分级配置

5.7.2.1配置分级配置任务序列

1. 进入特权模式命令
2. 设置登录身份的相关密码

1. 进入特权模式命令

命令	解释
Enable [level {visitor | admin} [<*password*>]]	用指定身份及密码登录交换机

2. 设置登录身份的相关密码

命令	解释
enable password level {visitor|admin}	指定登录配置模式的密码

5.7.2.2配置分级配置命令

5.7.2.2.1 Enable

命令：Enable [level {visitor|admin} [<*password*>]]
功能：可以指定登录用户的身份是管理级还是访问级。
参数：<*password*>：对应身份的登录密码
命令模式：一般用户模式
缺省情况：以admin身份登录
使用指南：系统设置了密码，登录没有输入密码时，将启动交互方式询问密码。
举例：以visitor身份进入特权模式，密码为dcn
方法一：
SWITCH>enable level visitor dcn
SWITCH#
方法二：
SWITCH >enable level visitor
Password:***　　　　　　　　　　<--------------输入dcn
SWITCH#

5.7.2.2.2 Enable password level

命令：Enable password level {visitor|admin}
功能：指定登录配置模式的密码
命令模式：config模式
缺省情况：无密码（当前密码为空）

使用指南：配置此命令，将启用交互方式询问
当前密码，新密码，确认新密码。密码可以为空。当新密码及确认新密码为空时，等于取消该登录身份的密码。

举例: 设置visitor身份的登录密码为dcn

SWITCH#enable password level visitor
Current password:
New password:*** <------------- 输入dcn
Confirm new password:*** <------------- 输入dcn

第6章 堆叠配置

6.1 堆叠介绍

6.1.1 堆叠协议介绍

堆叠（stack）协议是一种交换机管理技术，可将物理上的若干台交换机堆叠在一起，逻辑上当成一台交换机进行管理。根据交换机之间连接方式的不同，堆叠交换机有三种配置方式：

1. Simplex 方式：一台交换机的 TX 端口和另一台交换机的 RX 端口之间通过单向数据线连接，从而形成一个单向链路环。simplex 方式形成的堆叠组，每台交换机只需要一个全双工端口用于堆叠交换机之间的通讯。缺点是容错性较差，任何一条链路出现故障，都会造成堆叠组瘫痪。

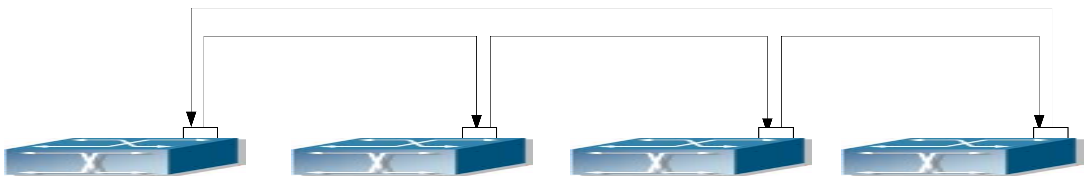


图 6-1 simplex 方式

2．Duplex 方式：交换机之间通过双向数据线连接形成双向两路环。duplex 方式形成的堆叠组，每台交换机必须两个全双工端口用于堆叠交换机之间的通讯。为避免形成数据环，堆叠协议把其中一条数据链路作为冗余链路，并设置为 passive 状态。Duplex 堆叠方式具有较好的容错性，如果一条数据链路出现故障，堆叠协议可以启用冗余链路进行通讯，从而可以保持堆叠组稳定运行。为节约级联端口，也可以取消冗余链路，而把交换机链接成为线形。

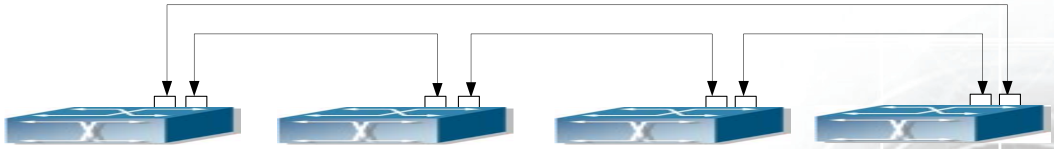


图 6-2 duplex 方式

3．chassis 方式：以一台高性能交换机作为 Master 形成星形。Chassis 堆叠方式，任一两台交换机之间进行通讯，都必需经过 Master 交换机。Master 交换机必须是一台处理能力较强的高性能交换机，否则容易形成通讯瓶颈。

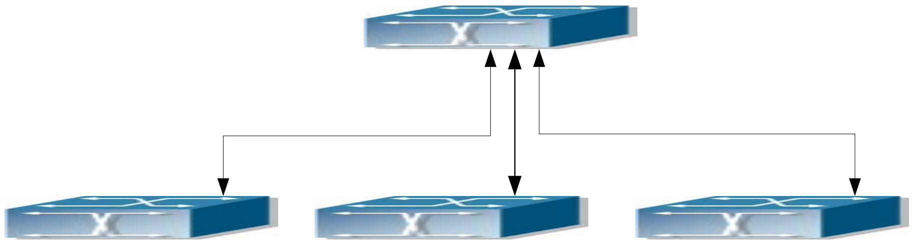


图 6-3 chassis 方式

目前交换机支持 simplex 和 duplex 两种堆叠方式。堆叠交换机启动后，首先运行 MDP（Master Discovery Protocol）或 DDP（Duplex Discover Protocol）选举一台交换机作为 Master，其它交换机作为 Slave。Master 负责管理所有 Slave 交换机，并负责为每台 Slave 分配一个 ID 号，Master 的 ID 为 0。

堆叠组稳定之后，Master 周期性的发出 HBP（Heart Beat Protocol）报文，查询 Slave 交换机的状态，并检测堆叠组的拓扑状态变化。Master 交换机和 Slave 交换机之间通过 RDP（Reliable Datagram Protocol）协议交换数据：Master 分发交换机配置参数并查询 Slave 的工作状态；Slave 报告其工作状态并转发接收到的协议报文。

交换机最多支持一个堆叠组内有 9 台堆叠交换机。如果堆叠交换机发现多于 9 台堆叠交换机连接在一起，所有交换机都工作于 STANDALONE 模式，无法形成有效的堆叠组。

6.1.2 确定 Master 和 Slave

在堆叠组稳定之后，观察堆叠灯的状态，堆叠灯一直点亮的交换机就是 Master，其他均为 Slave。在 Master 交换机上可查询堆叠组的参数信息，并可以通过点灯命令确定 Slave 交换机的 SWITCH ID。

6.1.3 堆叠组交换机的管理

堆叠交换机采用集中管理的方式，所有配置参数必须通过 Master 进行分发，所有协议状态机都在 Master 上计算和维护。Slave 交换机接收到协议报文后，通过 RDP 协议转发至 Master 交换机处理，Master 交换机把计算结果分发至相关 Slave 交换机。

Master 交换机把所有 Slave 交换机的物理端口均映射至 Master 的系统。堆叠交换机的端口位置信息分为三段（如 Ethernet1/0/5），第一段表示端口所在交换机的 SWITCH ID，第二段表示端口所在插槽的位置，第三段表示端口所在的物理位置。如端口 Ethernet1/0/5 表示，此端口为 Slave 1 的第一个端口插槽上的第五个端口在 Master 上的映射端口。

为了充分发挥堆叠交换机的性能，堆叠组内所有交换机独立维护二层，三层转发表项。静态 MAC 地址通过 Master 配置并分发至堆叠组内所有 Slave 交换机，动态 MAC 地址各个堆叠交换机独立学习，更新，并根据本地 MAC 地址表独立转发二层数据。三层接口在 Master 上配置并分发至所有三层交换机，路由协议在 Master 启动，并维护其状态机。Master 计算出路由后，分发至所有三层 Slave 交换机，使得堆叠组内的所有三层交换机具有统一的路由表项。三层堆叠交换机根据本地路由表和本地 IP 数据流独立设置三层转发表项。

6.2 堆叠配置

6.2.1堆叠配置任务序列

1. 配置堆叠模式和堆叠端口（必须）；
2. 配置堆叠交换机的优先级（可选）；
3. 重新启动交换机，使其启动堆叠协议（必须）；

1. 配置堆叠模式和堆叠端口

命令	解释
全局配置模式	
stacking enable {{{duplex|chassis} interface <*intf1*> [interface <*intf2*>]} | {simplex interface <*intf1*>}} **stacking disable**	使能堆叠协议工作模式和堆叠端口；disable 为关闭堆叠协议。

2. 配置堆叠交换机的优先级

命令	解释
全局配置模式	
stacking priority <*priority*> **no stacking priority**	配置堆叠交换机的堆叠优先级；本命令的 no 操作为恢复交换机的堆叠优先级为缺省值。

6.2.2 堆叠配置命令

6.2.2.1 stacking

命令：stacking enable {{{duplex|chassis} interface <*intf1*> [interface <*intf2*>]} | {simplex interface <*intf1*>}}
stacking disable

功能：使能堆叠协议工作模式并且指定堆叠端口；disable 为关闭堆叠协议。

参数：simplex、duplex、chassis 为堆叠交换机工作模式，目前交换机支持 simplex 和 duplex 两种堆叠方式；**<*intf1*>**、**<*intf2*>**为堆叠端口的名字。

命令模式：全局配置模式

缺省情况：缺省交换机工作于 STANDALONE 模式，没有端口参与堆叠工作。

使用指南：使能堆叠协议的交换机必须指定一个或者两个堆叠端口用于堆叠交换机之间的连接。堆叠端口必须是千兆端口。

注意：本命令必须重新启动交换机才能生效。本命令不可以追加配置堆叠端口，重新启动交换机后，最后一次配置的堆叠端口将工作于堆叠模式。

举例：配置交换机的两个扩展电口为堆叠端口，并工作于 duplex 堆叠模式。

Switch(Config)#stacking enable duplex interface ethernet0/1/1 interface ethernet0/2/1

6.2.2.2 stacking priority

命令：stacking priority <*priority*>

no stacking priority

功能：配置堆叠交换机的堆叠优先级；本命令的 no 操作为恢复交换机的堆叠优先级的缺省值。

参数：<*priority*>为堆叠交换机的堆叠优先级值，取值范围 1~255。

命令模式：全局配置模式

缺省情况：堆叠交换机的堆叠优先级与交换机的型号有关，DCRS-5526S 交换机堆叠优先级缺省值为 100；DCS-3926S 交换机堆叠优先级缺省为 50，DCS-3950S 交换机堆叠优先级缺省为 60。

使用指南：堆叠组刚刚启动时，通过 MDP 协议选举堆叠优先级最高的交换机作为 Master；如果两台交换机的优先级相等，则比较交换机的 CPU MAC 地址的大小，CPU MAC 地址大的交换机被选举为 Master。

举例：配置交换机的堆叠优先级为 200。

Switch(Config)#stacking priority 200

6.3 堆叠举例

案例：

四台交换机 SW1-SW4 采用 duplex 堆叠方式组成堆叠组，并确保 SW1 被选举为 Master。

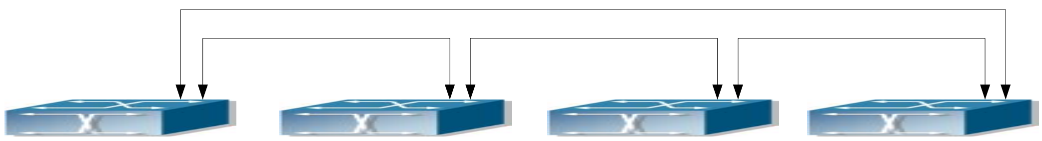


图 6-2 交换机堆叠

配置步骤：

1. 配置堆叠端口

SW1-SW4 的配置：

Switch(Config)#stacking enable duplex interface ethernet0/1/1 interface ethernet0/2/1

2. 配置 SW1 的堆叠优先级为 200（其它交换机的保持堆叠优先级的默认值 100）

SW1 的配置：

Switch(Config)#stacking priority 200

3. 重新启动 SW1-4。

6.4 堆叠排错帮助

6.4.1 堆叠调试和监测命令

6.4.1.1 light module

命令：light module <*modid*>
功能：点亮堆叠交换机的堆叠灯。
参数：<*modid*>为 SWITCH ID，取值范围为 0-8。
命令模式：特权用户配置模式
使用指南：在 Master 上执行此命令可以点亮 Slave 交换机的堆叠灯，从而帮助用户确定 Slave 交换机在整个堆叠组中的的 SWITCH ID。

6.4.1.2 show stacking

命令：show stacking
功能：显示堆叠相关的信息。
命令模式：特权用户配置模式
使用指南：在 Master 上执行此命令可以查询 Slave 交换机的堆叠信息，在 Slave 交换机上执行此命令只能查询本地堆叠信息。
举例：Switch#show stacking

```
Running:
        Mode: duplex
        Priority: 100
Flash config:
        Mode: duplex
        Priority: 100
        Port: Ethernet0/2/1

DDP state : HB STATE, stack unit : 0

Advertise: send 21, rcvd 0. Advertise ACK: send 0, rcvd 21
Heart Beat: send 31, rcvd 0. Heart Beat ACK: send 0, rcvd 31

Total number of switchs in stack : 2
My switch ID : 0 (master is 0)

Switch ID 1
Switch type DCS-3926S
Max number of:
        active vlan 255
        static mac 8191
```

```
            group mac 255
            L3 interface 1
Number of port 24
Left stack port: none
Right stack port: Ethernet0/2/1
Cpu Mac Addr: 0:3:f:1:c1:96
Priority 50
             number of chips 1 : (5615 modid 2)

Switch ID 0      <---- self
Switch type DCS-3926S
Max number of:
            active vlan 255
            static mac 8191
            group mac 255
            L3 interface 1
Number of port 24
Left stack port: Ethernet0/2/1
Right stack port: none
Cpu Mac Addr: 0:3:f:11:22:32
Priority 100
             number of chips 1 : (5615 modid 1)
```

显示信息	解释
Running	运行信息
Flash config	用户最后一次的配置
Mode	堆叠方式
Priority	堆叠优先级
Port	用户配置的堆叠端口
DDP state	堆叠协议运行状态
Advertise	堆叠发现包
Advertise ACK	堆叠发现包 ACK
Heart Beat	堆叠心跳包
Heart Beat ACK	堆叠心跳包 ACK
Total number of switchs in stack	堆叠组内交换机数目
My switch ID	本交换机堆叠 ID
switch ID	交换机的 ID
Switch type	交换机型号
active vlan	活动 VLAN 的数量
static mac	静态 MAC 地址的数量
group mac	组播 MAC 地址的数量
L3 interface	三层端口的数量
Number of port	物理端口的数量
Left stack port:	堆叠端口

Right stack port	堆叠端口

6.4.1.3 debug stacking

命令：debug stacking {rpc|ddp|rdp|mdp}
no debug stacking {rpc|ddp|rdp|mdp}
功能：打开堆叠的调试信息；本命令的 no 操作为关闭堆叠的调试信息。
参数：rpc 为 MASTE 通过 RPC（Remote Process Call）调用管理 Slave 交换机的运行状态；**ddp** 为 Master 通过 DDP（Duplex Discovery Protocol）监测 Duplex 堆叠组的拓扑状态；**rdp** 为 Master 交换机和 Slave 交换机之间通过 RDP（Reliable Datagram Protocol）进行通讯；**mdp** 为 Master 通过 MDP(Master Discovery Protocol)监测 Simplex 堆叠组的拓扑状态。
命令模式：特权用户配置模式
使用指南：Master 分发配置参数至 Slave 交换机时，首先把参数通过 RPC 协议封装为 RPC 报文格式，然后再调用 RDP 协议转发参数。堆叠协议为每种参数设置了 RPC ID，调试 RPC 信息，可以获知 Master 分发参数的执行状况；调试 DDP 信息，可以获知 Duplex 堆叠交换机发送和接收心跳报文的数量和时间；调试 RDP 信息，可以获知堆叠交换机发送 RDP 报文的数量，以及接收到 ACK 报文的数量；调试 MDP 信息，可以获知 Simplex 堆叠交换机发送和接收心跳报文的数量和时间。

6.4.2 堆叠排错帮助

当在是用堆叠组过程中遇到问题，请检查是否是如下原因：

- 堆叠组不断在重新启动，无法正常工作，请检查是否将堆叠交换机的堆叠端口和 STANDALONE 交换机的非堆叠端口互联了。由于工作于 STANDALONE 状态的交换机，可以透传堆叠协议报文，导致堆叠组的状态无法稳定。用户在使用时尽量避免此类事件发生。
- 无法在 Slave 交换机上配置参数。所有的配置参数只能在 Master 交换机上配置，不能直接在 Slave 交换机上配置。因此在 Slave 无法配置参数是正常的，用户只能在 Slave 交换机上执行查询和调试命令。
- 堆叠交换机只能在入口绑定 ACL，不能在出口绑定 ACL。

第7章 集群网管

7.1 集群网管介绍

集群网管是一种带内配置管理手段，与常规的 CLI、SNMP、Web Config 不同的是，它借助某台中间交换机（命令交换机）对目标交换机（成员交换机）进行间接配置管理，而不是在管理工作站上对目标交换机进行直接配置管理。命令交换机和成员交换机之间是一对多的关系，在一台命令交换机上可以配置和管理多台成员交换机。只要在命令交换机上配置公网 IP，集群中所有成员交换机均可不配置公网 IP 也可以被远程配置管理，在 IP 资源日益紧张的今天，集群网管的配置手段节省了 IP 地址资源。而且集群网管做到了动态地发现具有集群功能的交换机（候选交换机），管理员可以根据需要手动或自动把发现的候选交换机加入已建立的集群，成为集群的成员交换机，从而可以通过命令交换机对成员交换机进行所有的配置和管理操作。当多台成员交换机分布在不同的地理位置（典型情况如不同的楼层）时，集群网管的方便性是很明显的。集群网管还有一个优点就是带内管理，即不需要为配置管理成员交换机而建立专门的通信联接，而是直接利用命令和成员之间的中继联线，因而是非常节省网络资源的。

基于集群网管以上特征，集群网管主要有以下优点：

- 节省 IP 地址
- 简化配置管理任务
- 不受网络拓扑结构和距离的限制
- 自动发现和自动建立功能
- 在出厂默认配置下就可以通过集群网管管理多台交换机
- 支持对集群内任意一台交换机的升级和配置管理

7.2 集群网管基本配置

7.2.1集群网管配置任务序列

1. 启动或停止集群功能
2. 建立集群
   创建或删除集群
   配置集群中成员设备使用的私有 IP 地址池
   在集群中加入或删除一个成员
3. 在命令交换机上配置集群相关属性
   1) 使能或禁止自动加入集群
   2) 设置集群的心跳保持时间
   3) 设置集群中的交换机发送心跳包的时间间隔
   4) 清除命令交换机发现的提请集群注册的交换机列表

4. 在候选交换机上配置集群相关参数
   1) 设置发送集群注册包的时间间隔
5. 利用集群网管进行远程管理
   1) 远程配置管理
   2) 重起成员交换机
   3) 对成员交换机进行远程升级

1. 启动或停止集群功能

命令	解释
全局配置模式	
cluster run **no cluster run**	启动或停止交换机本设备的集群功能

2．建立集群

命令	解释
全局配置模式	
cluster commander <*cluster-name*> *[vlan<vlan-id>]* **no cluster commander**	创建或删除集群
cluster ip-pool<*commander-ip*> **no cluster ip-pool**	配置集群中成员设备使用的私有 IP 地址池
cluster member {candidate-sn <*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>] }[password <*pass*>] **no cluster member < *mem-id* >**	添加或删除集群成员

3．在命令交换机上配置集群相关属性

命令	解释
全局配置模式	
cluster auto-add enable **no cluster auto-add enable**	使能或禁止把新发现的候选交换机加入集群
cluster holdtime < second> **no cluster holdtime**	设置集群的心跳保持时间
cluster heartbeat <*interval*> **no cluster heartbeat**	设置集群中的交换机发送心跳包的时间间隔
clear cluster candidate table	清除命令交换机发现的候选交换机列表

4. 在候选交换机上配置集群相关参数

命令	解释
全局配置模式	
cluster register timer <*timer-value*> **no cluster register timer**	设置发送集群注册包的时间间隔

5. 利用集群网管进行远程管理

命令	解释
特权模式	
rcommand<mem-id>	在命令交换机上使用该命令对集群的成员交换机进行配置管理
rcommand commander	在成员交换机上使用该命令对命令交换机进行配置管理
cluster reset member<mem-id>	在命令交换机上使用该命令重起成员交换机
cluster update member <*mem-id*> <*src-url*> <*dst-url*> [ascii | binary]	在命令交换机上对成员交换机进行远程升级

7.2.2集群配置命令

7.2.2.1cluster run

命令：cluster run
no cluster run
功能：启动集群功能，该命令的 no 操作停止集群功能
参数：无
命令模式：全局配置模式
缺省情况：默认开启集群功能
使用指南:本命令启动集群任务，只有集群功能开启，才能执行一切集群相关命令。执行 no 命令,将关闭本设备集群功能
举例：本地交换机上关闭集群任务
Switch (Config)#no cluster run

7.2.2.2cluser register timer

命令：cluster register timer<time-value>
no cluster register timer
功能：设置发送集群注册包的时间间隔，该命令的 no 操作恢复为默认值
参数：*<timer-value>*取值范围是:30-65535，单位是秒。
命令模式：全局配置模式

缺省情况：默认值是 60 秒

使用指南：本命令设置发送集群注册包的间隔取值为<time-vale>

举例：设置发送集群注册包的间隔为 80

Switch(Config)#cluster register timer 80

7.2.2.3cluster ip-pool

命令：cluster ip-pool <*commander-ip*>

no cluster ip-pool

功能：配置集群中成员设备使用的私有 IP 地址池

参数：*<commander-ip>*是命令交换机的 IP 地址，点分十进制格式；ip 地址的最后一个字节的值小于（255-24）。

缺省情况：缺省没有配置私有 IP 地址池

命令模式：全局配置模式

使用指南：建立集群前，用户必须首先在命令交换机上设置集群的私有 IP 地址池（如果不设置此地址池，则不能建立集群），当候选交换机加入集群时，命令交换机为每个成员分配一个可以在集群范围内使用的私有 IP 地址，并分发给成员交换机，用于集群内部的通讯，以实现命令交换机队成员交换机的管理和维护。该命令只能在非集群成员交换机上使用。若集群已经建立，则用户不能修改 IP 地址池。此命令的 NO 命令只是将地址池配置清除，没有默认值可以恢复。

举例：配置集群中成员设备使用的私有 IP 地址池 ip-pool 为 192.168.1.64

Switch(config)#cluster ip-pool 192.168.1.64

7.2.2.4cluster commader

命令：cluster commander <*cluster-name*> [vlan <*vlan-id*>]

no cluster commander

功能: 使能一个命令交换机，创建一个集群，修改集群名称；该命令的 no 操作删除该集群

参数：*<cluster-name>*是创建的集群的名字。***<vlan-id>***是集群三层 Device 所属的 vlan，如果用户不输入该参数，则集群三层 Device 所属的 vlan 为 vlan1。

缺省情况：缺省情况下没有建立集群

命令模式：全局配置模式

使用指南：本命令指定该交换机的角色为命令交换机，创建一个集群。执行该命令前，必须首先配置集群私有 IP 地址池。如果在命令交换机上再次执行该命令则修改集群的名字，并分发到成员交换机上。如果在成员交换机上执行该命令，则返回错误。如果在在命令交换机上再次执行该命令时附带了新的 vlan id，则新的 vlan id 是无效的。

举例:在本交换机上指定为命令交换机,集群的名字为 dcn ,vlan-id 为 vlan2

Switch(config)#cluster commander dcn vlan 2

7.2.2.5cluster member

命 令 :cluster member {candidate-sn
<*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>]} [password <*pass*>]
no cluster member < *mem-id* >

功能：在命令交换机上，把候选交换机加入命令交换机创建的集群；该命令的 no 操作从集群中删除一个成员

参数说明：**<*mem-id*>**为成员的 ID，取值范围为：1-23；**<*cand-sn*>**是交换机在候选交换机列表中的编号，取值范围 0-127，允许使用‘；’和‘—’进行个别或连续选择编号。**<*mac-add*>**为成员交换机的 MAC 地址,格式为 XX-XX-XX-XX-XX-XX；**<*pass*>**为成员交换机的特权密码；

缺省情况：无

命令模式：全局配置模式

使用指南：命令交换机执行该命令后，把**<*mac-add*>**或**<*cand-sn*>**标示的交换机加入命令交换机所在的集群。如果在非命令交换机上运行该命令时，返回错误。

举例:在命令交换机上把候选交换机加入到集群中,候选交换机在候选列表中的编号为为 17,pass 为 mypassword

Switch(config)#cluster member candidate-sn 17 mypassword

7.2.2.6cluser auto-add

命令：**cluster auto-add enable**
no cluster auto-add enable

功能：在命令交换机上使能该命令以后，可以把新发现的候选交换机自动加入集群，成为集群的成员交换机；该命令的 no 操作禁止该操作。

参数说明：无

缺省情况：系统默认禁止该功能，即不自动把候选交换机加入集群。

命令模式：全局配置模式

使用指南：在命令交换机上使能该命令以后，当命令交换机监听到新的交换机发送的集群注册包将把它们自动加入集群。如果在非命令交换机上运行该命令，返回错误。

举例:在命令交换机上打开集群自动加入功能

Switch(config)#cluster auto-add enable

7.2.2.7rcommand member

命令：**rcommand member <*mem-id*>**

功能：在命令交换机上使用该命令对集群的成员交换机进行远程配置管理

参数说明：**<*mem-id*>**是成员交换机的集群 ID，取值范围：1-23。

缺省情况：无

命令模式：特权模式

使用指南：使用该命令直接进入成员交换机的特权模式，进行远程配置管理。使用 exit 退出成员交换机的配置界面。如果在非命令交换机上运行该命令，返回错误。

举例:在命令交换机上进入 mem-id 为 15 的成员交换机的配置界面

Switch#rcommand 15

7.2.2.8rcommand commander

命令：rcommand commander
功能：在成员交换机上使用该命令远程管理和配置命令交换机
参数说明：无
缺省情况：无
命令模式：特权模式
使用指南：执行该命令后可以对命令交换机进行远程管理和配置，但要通过命令交换机上的 telnet 用户名密码验证。使用 exit 退出命令交换机的配置界面。如果在命令交换机上运行该命令，返回错误。
举例: 在成员交换机上使用该命令进入命令交换机的配置界面
Switch#rcommand commander

7.2.2.9cluster reset member

命令：cluster reset member <*mem-id*>
功能：在命令交换机上使用该命令重起成员交换机
参数说明：<*mem-id*>是成员交换机的集群 ID，取值范围：1-23。可以使用连接号"-"和分号"；"输入多个**<*mem-id*>**。
缺省情况：无
命令模式：特权模式
使用指南：本命令使命令交换机分发重起命令到成员交换机，成员交换机重起。如果在非命令交换机上运行该命令，返回错误。
举例:在命令交换机上从新启动成员交换机 16
Switch#cluster reset member 16

7.2.2.10 cluster update member

命令：cluster update member <*mem-id*> <*src-url*> <*dst-url*> [ascii | binary]
功能:命令交换机上对成员交换机进行远程升级
参数说明：<*mem-id*>是成员交换机的集群 ID，取值范围：1-23。**<*src-url*>**为被拷贝的源文件或目录的位置；**<*dst-url*>**为文件或目录所要拷贝到的目的地址；**ascii** 表示文件传输使用 ASCII 标准；**binary** 表示文件传输使用二进制标准。当**<*src-url*>**是 FTP 地址时的格式为：ftp://<*username*>:<*password*>@<*ipadress*>/<*filename*>，其中<*username*>为 FTP 用户名，<*password*>为 FTP 用户口令，<*ipadress*>为 FTP 服务器的 IP 地址，<*filename*>为 FTP 下载文件名。当**<*src-url*>**是 TFTP 地址时的格式为：tftp://<*ipadress*>/<*filename*>，其中<*ipadress*>为 TFTP 服务器的 IP 地址，<*filename*>为 TFTP 下载文件名。

filename 的特殊关键字：

关键字	源地址或目的地址

startup-config	启动配置文件
nos.img	系统文件
nos.rom	系统启动文件

缺省情况：无
命令模式：特权模式
使用指南，命令交换机分发远程升级命令到成员交换机，成员交换机执行远程升级并重起。如果在非命令交换机上运行该命令则返回错误。
举例:在命令交换机上对成员交换机进行远程升级,成员交换机 mem-id 为 10 ， src-url 为 ftp://dcn:dcn@192.168.1.1/nos.img ，dst-url 为 nos.img
Switch#cluster update member 10 192.168.1.2 ftp://dcn:dcn@192.168.1.1/nos.img nos.img

7.2.2.11 cluster holdtime

命令：**cluster holdtime <*second*>**
no cluster holdtime
功能：在命令交换机上，使用该命令设置集群的心跳保持时间；该命令的 no 操作恢复默认值
参数说明：**<*second*>**为集群的心跳保持时间，取值范围：20～65535。心跳保持时间是指心跳包信息的最长有效时间，再次收到心跳包将刷新这个保持时间，如果在心跳保持时间内一直没有收到心跳包，则心跳包信息失效，即集群关系失效。
缺省情况：默认值为 80 秒
命令模式：全局配置模式
使用指南：命令交换机执行该命令后设置心跳保持时间为指定值，并分发到所有成员交换机。如果在非命令交换机上执行该命令或输入的 holdtime 取值小于等于当前心跳间隔取值，则设置无效，显示错误。
举例:设置集群心跳包保持时间为 100
Switch(config)#cluster holdtime 100

7.2.2.12 cluster heartbeat

命令：**cluster heartbeat <*interval*>**
no cluster heartbeat
功能：在命令交换机上，使用该命令设置集群中的交换机发送心跳包的时间间隔；该命令的 no 操作恢复默认值
参数说明：**<*interval*>**为集群的心跳时间间隔，取值范围：1-65535 秒，为整型
缺省情况：默认值为 8 秒
命令模式：全局配置模式
使用指南：命令交换机执行该命令后，设置心跳时间间隔为指定值，并分发到所有成员交换机上。如果在非命令交换机上执行该命令或输入的心跳间隔取值大于等于当前 holdtime 取值，则设置无效，显示错误

举例:设置集群发送心跳包时间间隔为 10
Switch(config)#cluster heartbeat 10

7.2.2.13 clear cluster candidate table

命令：**clear cluster candidate table**
功能：清除命令交换机发现的候选交换机列表。
参数说明:无
缺省情况：无
命令模式：特权模式
使用指南：本命令清除命令交换机发现的候选交换机列表。在非命令交换机执行该命令则返回错误。
举例: 清除命令交换机发现的候选交换机列表。
Switch#clear cluster candidate table

第8章 端口配置

8.1 端口介绍

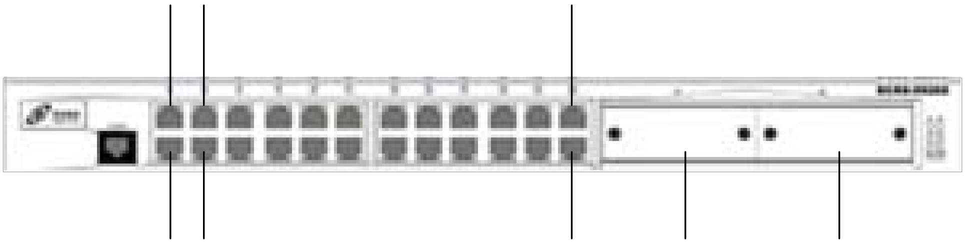


图 8-1 DCRS-5526S 端口示意图

DCRS-5526S 的端口配置如图所示。DCRS-5526S 提供 24＋2 个端口，其中 24 个为固定配置的 10/100Base-TX 以太网接口，2 个为可选模块 M1、M2。M1 和 M2 可以插入的端口类型有：1000Base-TX 以太网接口、10/100Base-TX 以太网接口、100Base-FX 单模/多模接口、1000Base-FX 单模/多模接口和堆叠接口。

在 DCRS-5526S 的面板上标注有各个端口的端口号，该端口号与 DCRS-5526S 操作系统提供的端口号（软件意义上的端口号）的对应关系如下：

物理端口号	软件端口号
24 个 10/100Base-T	ethernet 0/0/1-24
M1	ethernet 0/1/1
M2	ethernet 0/2/1

即如果用户要对某些端口进行配置，可以使用命令 **interface ethernet <*interface-list*>**进入到相应的以太网接口配置模式，参数**<*interface-list*>**为 0/0/1-24 或者 0/1/1、0/2/1，**<*interface-list*>**包含多个端口时，可以使用"；"和"-"等特殊字符进行连接，"；"连接不连续的端口号，"-"连接连续的端口号，其中 0/1/1、0/2/1 只能在扩展插槽 M1、M2 安装后才能使用。在以太网接口配置模式下可对端口的速率、双工模式、流量控制等进行配置，相应物理端口的表现也随之改变。

8.2 端口配置

8.2.1以太网端口配置

8.2.1.1以太网端口配置任务序列

1. 进入以太网接口配置模式
2. 配置以太网端口的属性
   （1） 打开或关闭端口
   （2） 配置端口名字
   （3） 配置端口连线类型
   （4） 配置端口速率
   （5） 配置端口双工模式
   （6） 配置带宽控制
   （7） 配置流量控制
   （8） 打开或关闭端口环回功能
3. 配置交换机广播风暴抑制功能

1. 进入以太网接口配置模式

命令	解释
接口配置模式	
interface ethernet <*interface-list*>	进入以太网接口配置模式。

2. 配置以太网端口的属性

命令	解释
接口配置模式	
shutdown **no shutdown**	关闭或打开指定端口。
name <*string*> **no name**	设定或取消设定指定端口的名字。
mdi { auto | across | normal } **no mdi**	设置指定端口的连线类型；本命令的 no 操作为恢复默认连线类型。
Speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }	设置端口的速率和双工模式。
bandwidth control <*bandwidth*> [both | receive | transmit] **no bandwidth control**	设置指定端口收、发数据占用的带宽。
flow control **no flow control**	打开或关闭指定端口的流量控制功能。
loopback **no loopback**	打开或关闭指定端口的环回测试功能。

3. 设置广播风暴抑制功能

命令	解释
全局配置模式	
broadcast-suppression <*packets*> **no broadcast-suppression**	打开交换机的广播风暴抑制功能，并设置允许通过的广播流量；本命令的 no 操作为取消广播风暴抑制功能。

8.2.1.2以太网端口配置命令介绍

8.2.1.2.1 bandwidth

命令：bandwidth control <*bandwidth*> [both | receive | transmit]
　　no bandwidth control
功能：打开端口的带宽限制功能；本命令的 no 操作为关闭端口的带宽限制功能。
参数：<*bandwidth*>为限制带宽，单位为 Mbps，取值范围为 1-1000M；**both** 为端口收发时均进行带宽控制；**receive** 为仅在端口接收数据时进行带宽控制；**transmit** 为仅在端口发送数据时进行带宽控制。
命令模式：接口配置模式
缺省情况：端口缺省关闭带宽控制功能。
使用指南：当端口设置了带宽限制功能，并且指定了限制带宽的大小，那么端口的最大带宽就被确定，而不以 10/100M 为最大带宽。如果不指定**[both | receive | transmit]**关键字，缺省为 **both**。
举例：设置 1-8 号端口限制带宽为 40M。
Switch(Config)#interface ethernet 0/0/1-8
Switch(Config-Port-Range)#bandwidth control 40 both

8.2.1.2.2 broadcast-suppression

命令：broadcast-suppression <*packets*>
　　no broadcast-suppression
功能：设置交换机所有端口允许通过的广播流量；本命令的 no 操作为关闭端口抑制广播风暴功能，即允许线速通过广播流量。
参数：<*packets*>代表每秒钟允许通过的广播数据报的个数，取值范围为 1~262143。
命令模式：全局配置模式
缺省情况：缺省允许线速通过广播流量。
使用指南：在没有任何 VLAN 设置的情况下，交换机的所有端口都处在同一个广播域，广播流量的产生极其影响交换机的性能，打开交换机的广播风暴抑制功能，可以保护交换机尽量少地受广播风暴的影响。当设置端口允许通过的广播流量为 3 时，表示当端口每秒钟接收的广播数据报大于 3 时，多于 3 的部分将被抑制。
DCRS-5526S 不仅抑制广播流量，也可以抑制组播流量和在 MAC 地址表中不存在的单播流量。
举例：交换机所有端口最多允许每秒钟通过 3 个广播数据报。
Switch(Config)#broadcast-suppression 3

8.2.1.2.3 flow control

命令：flow control

no flow control

功能：打开指定端口的流控功能；本命令的 no 操作为关闭端口的流控功能。

命令模式：接口配置模式

缺省情况：端口的流控功能缺省为关闭。

使用指南：打开端口的流控功能后，当端口接收到的流量大于端口缓存所能容纳的大小时，端口将通过算法或者协议通知向其发送流量的设备减慢发送速度，以防止丢包。交换机的端口工作在全双工模式下，支持 802.3X 流量控制；端口工作在半双工模式下，支持背压流控。

注意：在打开端口的流控功能时，请务必确认两端的速率和双工模式相同。

举例：打开 0/0/1-8 号端口的流控功能。

Switch(Config)#interface ethernet 0/0/1-8

Switch(Config-Port-Range)#flow control

8.2.1.2.4 interface ethernet

命令：interface ethernet <*interface-list*>

功能：从全局配置模式进入到以太网接口配置模式。

参数：<*interface-list*>为端口号，端口号的格式和取值范围见本章端口介绍部分的说明。

命令模式：全局配置模式

使用指南：使用命令 **exit** 可从以太网接口配置模式退回到全局配置配置。

举例：进入以太网端口 0/0/1，0/0/4-5，0/0/8。

Switch(Config)#interface ethernet 0/0/1;0/0/4-5;0/0/8

Switch(Config-Port-Range)#

8.2.1.2.5 loopback

命令：loopback

no loopback

功能：设置以太网端口进行环回测试功能；本命令的 no 操作用来取消以太网端口的环回测试。

缺省情况：以太网端口不进行环回测试。

命令模式：接口配置模式

使用指南：使用环回测试可以检验以太网端口是否正常工作

举例：设置以太网端口 0/0/1-8 进行环回测试。

Switch(Config)#interface ethernet 0/0/1-8

Switch(Config-Port-Range)#loopback

8.2.1.2.6 mdi

命令：mdi { auto | across | normal }

no mdi

功能：设置指定以太网端口连接的以太网连线类型；本命令的 no 操作为恢复以太网端口缺省连接的以太网线类型。

参数：auto 为自动协商连接的以太网线类型；**across** 为以太网线类型为交叉线；**normal** 为以太网类型为直连线。

命令模式：接口配置模式

缺省情况：端口缺省自动协商连接的以太网线类型。

使用指南：本命令仅限于固定端口使用，固定端口缺省是自动协商以太网线的类型，用户可以不必关心以太网线是交叉线还是直连线、对端设备是主机还是交换机，只要以太网线和对端设置的网卡是可用的，DCRS-5526S 就能保证与之正确连接。

举例：设置 0/0/1-8 号端口连接的网线为交叉线。

Switch(Config)#interface ethernet 0/0/1-8

Switch(Config-Port-Range)#mdi across

8.2.1.2.7 name

命令：name <*string*>

no name

功能：为指定的端口设置名字；本命令的 no 操作为取消该项配置。

参数：<*string*>为字符串，最长不超过 200 个字符。

命令模式：接口配置模式

缺省情况：端口缺省没有名字。

使用指南：本命令有助于用户管理交换机，如用户可以根据端口的使用情况设置名字，如 1-8 号端口归财务部门使用，则定义为 finacial，9-20 号端口归工程部门使用，则定义了 egneering，21-24 号端口连接服务器，则定义 Servers。这样端口的使用情况就一目了然了。

举例：指定 0/0/1-8 端口 name 为 finacial。

Switch(Config)#interface ethernet 0/0/1-8

Switch(Config-Port-Range)#name finacial

8.2.1.2.8 shutdown

命令：shutdown

no shutdown

功能：关闭指定的以太网端口；本命令的 no 操作为打开端口。

命令模式：接口配置模式

缺省情况：以太网端口缺省为打开。

使用指南：当关闭以太网端口时，以太网端口将不发送数据帧，并且在 **show interface** 时显示端口状态为 down。

举例：打开 0/0/1-8 号端口。

Switch(Config)#interface ethernet 0/0/1-8

Switch(Config-Port-Range)#no shutdown

8.2.1.2.9 speed-duplex

命令：speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }
no speed-duplex
功能：设置端口的速率和双工模式，本命令的 no 操作恢复速度双工的默认值，即自动协商速度和双工(auto)。
参数：auto 为自动协商速率；**force10-half** 为强制 10Mbit/s 速率，半双工模式；**force10-full** 为强制 10Mbit/s 速率，全双工模式；**force100-half** 为强制 100Mbit/s 速率，半双工模式；**force100-full** 为强制 100Mbit/s 速率，全双工模式；**force1g-half** 为强制 1000Mbit/s 速率，半双工模式；**force1g-full** 为强制 1000Mbit/s 速率，全双工模式；**nonegotiate** 为强制关闭千兆端口自动协商；**master** 为强制千兆端口为 master 模式；**slave** 为强制千兆端口为 slave 模式。
命令模式：端口配置模式。
缺省情况：端口缺省为自动协商速率和双工模式(auto)。
使用指南：在配置端口的速率和双工模式时，端口的速率和双工模式必须和对端设备速率和双工模式保持一致，即如果对端设备自动协商方式则本端也设置成自动协商方式；如果对端是强制方式，则本端也应设置成相应的强制方式。
对于千兆端口，配置**nonegotiate**方式时，默认为**master**。如果一端配置为**master**方式，另外一端必需配置为**slave**方式。
目前不支持**force1g-half**的配置。
举例：交换机 Switch1 端口 1 同交换机 Switch2 端口 1 用线相连，将该两个端口设置为强制 100Mbit/s 速率，半双工模式。
Switch1(Config)#interface e1/1
Switch1(Config-Ethernet1/1)#speed-duplex force100-half
Switch2(Config)#interface e1/1
Switch2(Config-Ethernet1/1)#speed-duplex force100-half

8.2.2 VLAN 接口配置

8.2.2.1 VLAN 接口配置任务序列

1. 进入 VLAN 接口配置模式
2. 配置 VLAN 接口的 IP 地址并打开 VLAN 接口

命令	解释
全局配置模式	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	进入 VLAN 接口配置模式，或删除已存在的 VLAN 接口。

1. 进入 VLAN 接口配置模式

2. 配置 VLAN 接口的 IP 地址并打开 VLAN 接口

命令	解释

VLAN 接口配置模式	
ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	配置 VLAN 接口的 IP 地址。
VLAN 接口配置模式	
shutdown **no shutdown**	打开或关闭 VLAN 接口。

8.2.2.2 VLAN 接口配置命令介绍

8.2.2.2.1 interface vlan

命令：interface vlan <*vlan-id*>
　　　no interface vlan <*vlan-id*>
功能：进入 VLAN 接口配置模式；本命令的 no 操作为删除已存在的 VLAN 接口。
参数：<*vlan-id*> 是已建立的 VLAN 的 VLAN ID，取值范围：1~4094。
命令模式：全局配置模式
使用指南：如果在配置 VLAN 接口的时候，已经存在一个 VLAN 接口，应先删除已有的 VLAN 接口。使用命令 **exit** 可以从 VLAN 接口配置模式退回到全局配置模式。
举例：进入 VLAN 1 接口配置模式。
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#

8.2.2.2.2 ip address

命令：ip address <*ip-address*> <*mask*> [secondary]
　　　no ip address [<*ip-address*> <*mask*>] [secondary]
功能：设置交换机的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。
参数：<*ip-address*>为 IP 地址，点分十进制格式；**<*mask*>**为子网掩码，点分十进制格式；**[secondary]**为表示配置的 IP 地址为从 IP 地址。
命令模式：VLAN 接口配置模式
缺省情况：系统缺省没有 IP 地址配置。
使用指南：本命令在 VLAN 接口手工配置 IP 地址，若没有配置可选参数 secondary，表示配置为 VLAN 接口的主 IP 地址，若配置了可选参数 secondary，则表示该 IP 地址为 VLAN 接口的从 IP 地址。交换机只能有一个主 IP 地址，可以有多个从 IP 地址。主 IP 和从 IP 均可以用于 SNMP/Web/Telnet 管理。此外，DCRS-5526S 还提供了 BOOTP/DHCP 方式获取 IP 地址。
举例：交换机的 IP 地址设置为 192.168.1.10/24。
Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

8.2.2.2.3 shutdown

命令：shutdown

no shutdown

功能：关闭交换机的 VLAN 接口；本命令的 no 操作为打开 VLAN 接口。

命令模式：VLAN 接口配置模式

缺省情况：VLAN 接口缺省为打开。

使用指南：当关闭交换机的 VLAN 接口，VLAN 接口将不发送数据帧。如果交换机在通过 BOOTP/DHCP 协议获取 IP 地址时，VLAN 接口是关闭的，那么交换机将得不到 IP 地址；要通过 BOOTP/DHCP 协议得到 IP 地址，必须将 VLAN 接口打开。

举例：打开交换机的 VLAN 接口。

Switch (Config-If-Vlan1)#no shutdown

8.2.3端口镜像配置

8.2.3.1端口镜像介绍

端口镜像功能是指交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口。通常在镜像目的端口处连接一个协议分析仪（如 Sniffer）或者 RMON 监测仪，可以监视和管理网络，并且能诊断网络故障。

DCRS-5526S 目前只支持一个镜像目的端口，镜像源端口则没有使用上的限制，可以是 1 个也可以是多个，多个源端口可以在相同的 VLAN，也可以在不同 VLAN。但如果镜像目的端口要能镜像到多个镜像源端口的流量，镜像目的端口必须要同时属于这些镜像源端口的所在的 VLAN。

端口镜像的模式共有两类：global 和 local。

其中：

global 模式是指在堆叠模式下，支持端口的跨堆叠的端口镜像，即镜像的源端口和目的端口可以不在同一台交换机上。需要指出的是：目前我们只支持只能配置一个 global 模式的端口镜像。而且只能在 simplex 堆叠的模式下才能配置 global 的镜像模式，不支持在 duplex 模式下的端口镜像。

local 模式是指在堆叠模式下，支持在同一台交换机上配置的端口镜像，可以在 master 上对堆叠中的各个交换机，进行端口镜像的配置，可以配置多个 local 模式的端口镜像，但是每一台交换机同样只能配置一个镜像的目的端口；同一台交换机上只能配置一个端口镜像。

这两类模式是互斥的，也就是说不能同时配置 global 和 local 的端口镜像模式。

8.2.3.2端口镜像配置任务序列

1. 指定镜像源端口
2. 指定镜像目的端口

1. 指定镜像源端口

命令	解释
全局配置模式	
monitor session <*session*> source interface {[ethernet]<*interface-list*>} {rx| tx| both} **no monitor session <*session*> source interface {[ethernet]<*interface-list*>}**	指定镜像源端口；本命令的 no 操作为删除镜像源端口。

2. 指定镜像目的端口

命令	解释
全局配置模式	
monitor session <*session*> destination interface {[ethernet]<*interface-number*>} **no monitor session <*session*> destination interface <*interface-number*>**	指定镜像目的端口；本命令的 no 操作为删除镜像目的端口。

8.2.3.3端口镜像配置

8.2.3.3.1 monitor session source interface

命令：monitor session <*session*> source interface{[ethernet] <*interface-list*>} {rx| tx| both}

no monitor session <*session*> source interface {[ethernet]<*interface-list*>}

功能：指定镜像源端口；本命令的 no 操作为删除镜像源端口。

参数：*<session>*为镜像 session 值，取值范围 1~100；但根据堆叠组的数目，目前最多只能支持 9 个 session（在全部为 local 的情况下）；从 session 取值中无法辨别 global 方式，还是 local 方式，两种方式采用 session 号统一编号。***<interface-list>***为镜像源端口列表，支持 "-""；"等特殊字符；**rx** 为镜像源端口接收的流量；**tx** 为镜像从源端口发出的流量；**both** 为镜像源端口入和出的流量。

命令模式：全局配置模式

使用指南：本命令设置镜像的源端口，DCRS-5526S 对镜像源端口没有限制，可以是一个端口，也可以是多个端口，不仅能镜像源端口的发出和接收双向的流量，还能单独镜像源端口的发出流量及接收流量。如果不指定**[rx|tx|both]**关键字，缺省为 **both**。

说明：互相配对的源和目的端口的 session 值必须是相同的。

举例：设置镜像源端口为 0/0/1-4 的发出流量。

Switch(Config)#monitor session 1 source interface ethernet 0/0/1-4 tx

8.2.3.3.2 monitor session destination interface

命令：monitor session <*session*> destination interface {[ethernet]<*interface-number*>}

no monitor session <*session*> destination interface {[ethernet]<*interface-number*>}

功能：指定镜像目的端口；本命令的 no 操作
为删除镜像目的端口。

参数：***<session>***为镜像 session 值，取值范围 1~100；但根据堆叠组的数目，目前最多只能支持 9 个 session（在全部为 local 的情况下）；从 session 取值中无法辨别 global 方式，还是 local 方式，两种方式采用 session 号统一编号。***<interface-number>***为镜像目的端口。

命令模式：全局配置模式

使用指南：DCRS-5526S 目前仅支持一个镜像目标端口。需要注意的是，作为镜像目标端口不能是端口聚合组的成员，并且端口吞吐量最好大于或等于它所镜像的所有源端口的吞吐量的总和。

说明：互相配对的源和目的端口的 session 值必须是相同的。

举例：设置镜像目的端口为 0/0/7。

Switch(Config)#monitor session 1 destination interface ethernet 0/0/7

8.2.3.4端口镜像举例

见端口配置举例。

8.2.3.5端口镜像排错帮助

8.2.3.5.1 show monitor

命令：show monitor

功能：显示镜像源、目的端口的信息。

命令模式：特权模式

使用指南：通过本命令可以显示当前设置的镜像源端口及目的端口。

举例：

Switch#show monitor

8.2.3.5.2 debug mirror

命令：debug mirror

no debug mirror

功能：打开 mirror 的调试信息；本命令的 no 操作为关闭 mirror 的调试信息。

命令模式：特权用户配置模式

使用指南：MASTER 分发配置参数至 SLAVE 交换机时，会显示相应的配置 mirror 的信息，使用户明白是否已经配置上相应的镜像。

8.2.3.5.3 端口镜像排错帮助

当配置端口镜像功能出现问题时，请检查是否是如下原因：

- 镜像目的端口是端口聚合组成员；如果是，请修改端口聚合组；
- 镜像目的端口的吞吐量小于镜像源端口吞吐量的总和，目的端口无法完全复制源端口的流量；请减少源端口的个数或复制单向的流量，或者选择吞吐量更大的端口作为目的端口。

8.3 端口配置举例

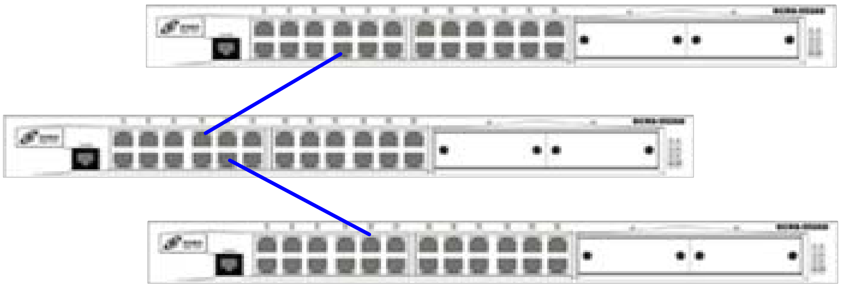


图 8-2 端口配置举例

交换机中均未配置 VLAN，因此使用缺省 VLAN1。

交换机	端口	属性
SW1	0/0/7	10M/full
SW2	0/0/8-9	10M/full、端口镜像源端口
	0/0/24	100M/full、端口镜像目的端口
SW3	0/0/10	10M/full

配置如下：

SW1：

Switch1(Config)#interface ethernet 0/0/7

Switch1(Config-Ethernet0/0/7)#speed-duplex force10-full

SW2：

Switch2(Config)#interface ethernet 0/0/8-9

Switch2(Config-Port-Range)# speed-duplex force10-full

Switch2(Config-Port-Range)#exit

Switch2(Config)#interface ethernet 0/0/24

Switch2(Config-Ethernet0/0/24)# speed-duplex force100-full

Switch2(Config-Ethernet0/0/24)#exit

Switch2(Config)#monitor session 1 source interface ethernet 0/0/8-9

Switch2(Config)#monitor session 1 destination interface ethernet 0/0/24

SW3：

Switch3(Config)#interface ethernet 0/0/10

Switch3(Config-Ethernet0/0/7)# speed-duplex force10-full

8.4 端口排错帮助

8.4.1监测和调试命令

8.4.1.1 clear counters ethernet

命令：clear counters [ethernet <*interface-list*>]
功能：清除以太网端口的统计信息。
参数：<*interface-list*>是以太网端口号。
命令模式：特权模式
缺省情况：缺省不会删除以太网端口的统计信息。
使用指南：如果不指定端口，则删除所有端口的统计信息。
举例：清除以太网端口 0/0/1 的统计信息。
Switch#clear counters ethernet 0/0/1

8.4.1.2 show interface ethernet

命令：show interface ethernet <*interface-list*>
功能：显示指定交换机端口的信息。
参数：<*interface-list*>为端口号，端口号的格式和取值范围见本章端口介绍部分的说明。
命令模式：特权模式
使用指南：本命令显示端口速率、双工模式、流控开关情况、广播风暴抑制以及收发数据包的统计情况。
举例：显示端口 0/0/1 的信息。
Switch#show interface ethernet 0/0/1

8.4.2端口排错帮助

用户在进行端口配置时通常会遇到的情况及解决建议如下：

☞ 输入 interface ethernet 0/1/1 时，提示出错。可能的原因是在 M1 和 M2 中没有插入扩展模块。需要注意的是如果用户仅在 M2 上插上了扩展模块，那么该模块对应的软件接口为 ethernet 0/2/1，而非 ethernet 0/1/1，输入 interface ethernet 0/1/1 时会提示出错。

第9章 MAC 地址表

9.1 MAC 地址表介绍

MAC 地址表是标识目的 MAC 地址与交换机端口之间映射关系的表，其 MAC 地址分为静态 MAC 地址和动态 MAC 地址。静态 MAC 地址由用户配置，具有最高优先级（不能被动态 MAC 地址覆盖）且永久生效；动态 MAC 地址由交换机在转发数据帧的过程中学习，且在有限时间内生效。当交换机接收到需要转发的数据帧时，首先学习数据帧的源 MAC 地址与接收端口之间的关系，并根据目的 MAC 地址查询 MAC 地址表。如果命中相关表项，交换机将数据帧从相应端口转发；否则，交换机将数据帧在其所属广播域内广播。如果动态 MAC 地址长时间没有被转发数据帧命中，交换机就将其从 MAC 地址表中删除。

对于 MAC 地址表的操作可分为两步：

1. MAC 地址的获取；
2. 根据 MAC 地址表转发或过滤。

9.1.1MAC 地址表的获取

MAC 地址表的获取可分为静态配置和动态学习。静态配置即由用户人为的建立 MAC 地址与端口的映射关系；动态学习即由交换机动态的发现 MAC 地址与端口的映射，并定期的更新 MAC 地址表。下面我们将重点介绍 MAC 地址表的动态学习过程。

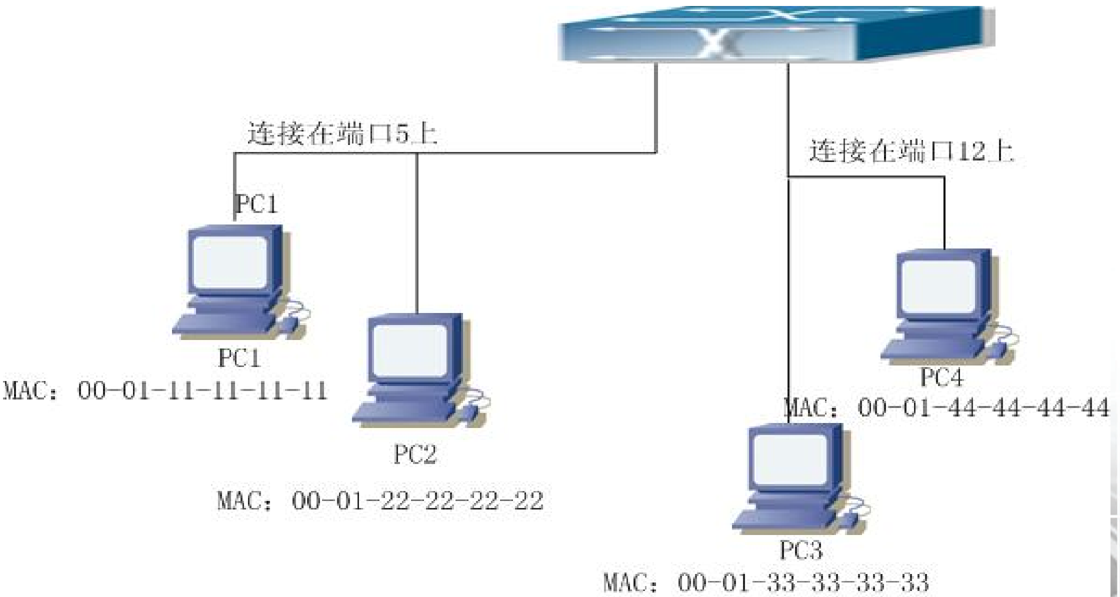


图 9-1 MAC 地址表动态学习

上图的拓扑环境为：4台主机连接在神州数码交换机上，其中主机1、2在同一个物理分

段中（即相同的冲突域），该物理分段与神州数码交换机的端口5相连；主机3、4在同一个物理分段，该物理分段与神州数码交换机的端口12相连。

初始状态下MAC地址表中没有任何学习到的地址映射表项，以主机1和主机3的相互通信为例，MAC地址表的学习过程如下：

1. 当主机1向主机3传输信息时，交换机在端口5处收到该信息的源MAC地址00-01-11-11-11-11，交换机的MAC地址表中就会增加MAC地址00-01-11-11-11-11和端口5映射表项；
2. 同时交换机会检查到该信息的目标MAC地址00-01-33-33-33-33，此时交换机中只有MAC地址00-01-11-11-11-11和端口5的映射表项，没有00-01-33-33-33-33对应的端口映射，因此交换机只能将该信息广播给交换机的每个端口；
3. 位于端口12的主机3、4均收到主机1发出的信息，但主机4不会给主机1回应，因为目标MAC地址为00-01-33-33-33-33，只有主机3会给主机1回应。这时交换机的12号端口收到主机3的发出的信息，交换机的MAC地址表中就又增加了MAC地址00-01-33-33-33-33和端口12映射表项；
4. 目前MAC地址表的内容为MAC地址00-01-11-11-11-11动态对应着端口5，MAC地址00-01-33-33-33-33动态对应着端口12。
5. 经过一段时间的主机1和主机3的通信之后，交换机再也没有接收到从主机1或者主机3发出的信息，300秒后交换机的MAC地址表将删除上面保存的MAC地址映射表项。这里的300秒是神州数码交换机缺省的MAC地址的老化时间，神州数码交换机提供老化时间的修改。

9.1.2转发或过滤

交换机会根据MAC地址表对接收到的数据帧做出转发或过滤的决定。以图上图为例，假设当前神州数码交换机MAC地址表动态学习到了主机1和主机3的MAC地址，用户又手工配置了主机2和主机4与端口的映射关系，此时的MAC地址表为：

MAC地址	端口号	获取方式
00-01-11-11-11-11	5	动态
00-01-22-22-22-22	5	静态
00-01-33-33-33-33	12	动态
00-01-44-44-44-44	12	静态

1. 根据MAC地址表转发的情况

如果主机1向主机3发送信息时，交换机根据MAC地址表，将该信息从端口5接收到的数据从端口12发出。

2. 根据MAC地址表过滤的情况

如果主机1向主机2发送信息，交换机根据MAC地址表，检查到主机2和主机1在同一个物理分段中，交换机将对该信息进行过滤，即不发送帧信息。

另外交换机能转发三种类型的帧：

- ✧ 广播帧。
- ✧ 组播帧；
- ✧ 单播帧。

下面简单介绍交换机对三种帧的处理：

1. 广播帧：交换机能阻隔冲突域，但不能阻
   隔广播域，在没有设置VLAN的情况下连接在交换机的所有设备是处在同一个广播域中的，当交换机接收到广播帧时，它会向所有的端口转发该广播帧。当交换机设置了VLAN后，MAC地址表也会做相应的调整，会增加VLAN的信息，此时交换机接收到广播帧后，不会将该广播帧转发给交换机内的所有端口，而是改变为只向属于同一个VLAN的所有端口转发。
2. 组播帧：当交换机没有设置IGMP Snooping的功能时，交换机对组播处理与广播的处理一样；当交换机设置IGMP Snooping功能时，交换机只会向属于该组播组的端口转发该组播帧。
3. 单播帧：在没有设置VLAN的情况下，当交换机的接收到的单播帧的目标MAC地址在MAC表中存在，交换机会直接将该单播帧转发到相应的端口；当接收到单播帧的目标MAC地址在MAC地址表中不存在时，交换机会对该单播帧进行广播。当交换机设置了VLAN，交换机只会在同一VLAN内转发单播帧；当转发单播帧的目标MAC地址在MAC地址表中存在，但不属于同一VLAN，此时交换机只能将该单播帧在它属于的VLAN内进行广播。

9.2 MAC 地址表配置

9.2.1mac-address-table aging-time

命令：mac-address-table aging-time {<*age*>| 0}

no mac-address-table aging-time

功能：设置 MAC 地址表中动态学习到的地址映射表项的老化时间；本命令的 no 操作为恢复系统的缺省老化时间 300 秒。

参数：<*age*>为老化时间，单位为秒，取值范围为 10～100000；**0** 为不老化。

命令模式：全局配置模式

缺省情况：系统缺省老化时间为 300 秒。

使用指南：老化时间设置的过小，交换机中会增加很多不必要广播影响性能；老化时间设置的过大，又会使一些早已不用的表项长期存在于 MAC 地址表中。因此用户应该根据实际情况合理的设置老化时间。

当老化时间设置为 0 秒时，交换机动态学习到地址就不会随着时间而老化，动态学习到的地址将一直保存在 MAC 地址表中。

注意：神州数码交换机的动态 MAC 地址实际老化时间是设置值的 1~1.5 倍之间的值，若在此期间没有接收到来自动态 MAC 地址的数据流，这些动态 MAC 地址将被老化。

举例：设置 MAC 地址表动态学习到的 MAC 地址的老化时间为 400 秒。

Switch(Config)#mac-address-table aging-time 400

9.2.2mac-address-table

命令：mac-address-table static address <*mac-addr*> vlan <*vlan-id* > interface [Ethernet|port-channel]<*interface-name*>

no mac-address-table [static| dynamic] [address <*mac-addr*>] [vlan <*vlan-id*>]

[interface <*interface-name*>]
功能：添加或修改静态地址表项，此命令的 no 操作为删除静态地址表项
参数：static 静态表项； **<*mac-addr*>** 要添加或删除的 MAC 地址；**<*interface-name*>** 转发 MAC 数据包的端口名称；**<*vlan-id*>** 接收 mac 地址数据包的 vlan 号。
命令模式：全局配置模式
缺省情况：当配置 VLAN 接口或三层接口后，系统会生成一个 VLAN 接口或三层接口与交换机固有的 MAC 地址的静态地址映射表项。
使用指南：在某些特殊用途或者交换机不能动态的学习到 MAC 地址，用户可以使用本命令将 MAC 地址与端口及 VLAN 手工建立映射关系。当端口类型为一个 **port-channel 时，**该 port-channel 必须是 up 的。
命令 **no mac-address-table** 为删除交换机 MAC 地址表中存在的所有动态、静态、过滤 MAC 地址表项，系统缺省保留的映射表项除外。
举例：端口 0/0/5 属于 VLAN200，与 MAC 地址为 00-03-0f-f0-00-18 建立地址映射。
Switch(Config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 0/0/5

9.2.3mac-address-table blackhole

命令：mac-address-table blackhole address <*mac-addr*> vlan <*vlan-id* >
no mac-address-table blackhole [address <*mac-addr*>] [vlan <*vlan-id*>]
功能：添加或修改过滤地址表项，此命令的 no 操作为删除过滤地址表项。
参数： **<*mac-addr*>** 要添加或删除的 MAC 地址； **<*vlan-id*>** 接收 mac 地址数据包的 vlan 号。
命令模式：全局配置模式
缺省情况：无过滤表项
使用指南：配置过滤表项的目的是丢弃指定 MAC 地址的帧，用于过滤不想让其通过的流量，可以过滤源地址和目标地址；过滤表项只与 Vlan 和 Mac 相关，与端口无关
举例：在 VLAN200，将 MAC 地址 00-03-0f-f0-00-18 设置为过滤表项。
Switch(Config)#mac-address-table blackhole address 00-03-0f-f0-00-18 vlan 200

9.3 典型配置举例

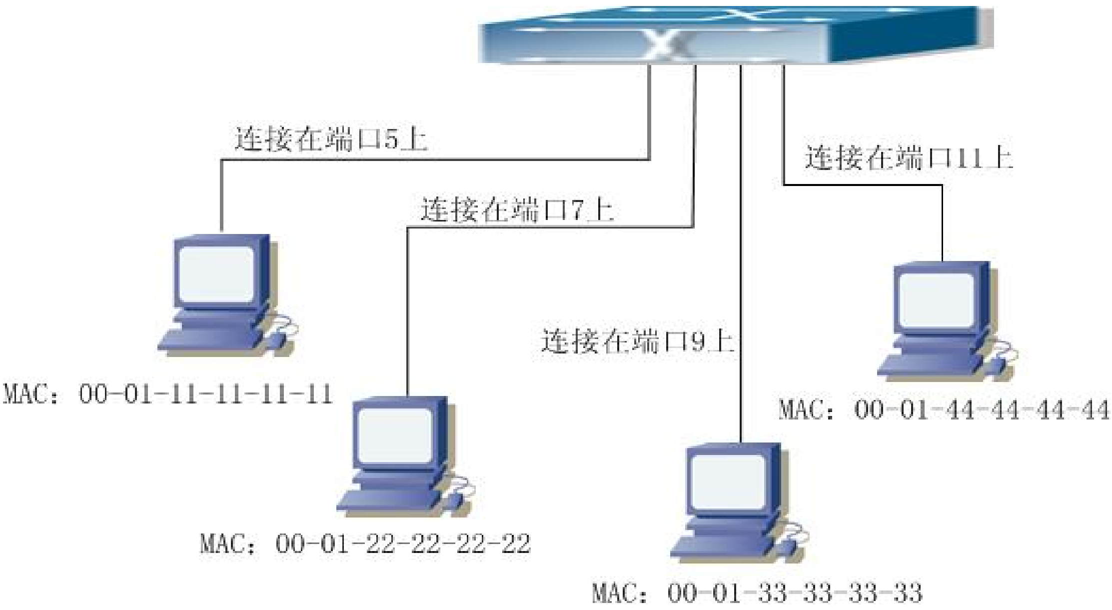


图 9-2 MAC 地址表典型配置举例

案例：如上图所示四台主机分别连接在神州数码交换机的 5、7、9、11 端口，这四台主机都属于缺省 VLAN1。根据实际网络的需要，动态学习功能是打开的；主机 1 保存有机密资料，任何与它不在一个物理分段的主机不能访问它；主机 2 和主机 3 分别与端口 7 和 9 建立静态映射关系。

配置步骤如下：

1.设置主机 1 的 MAC 地址 00-01-11-11-11-11 为过滤地址；

Switch(Config)#mac-address-table blackhole address 00-01-11-11-11-11 vlan 1

2.主机 2 和主机 3 分别与端口 7 和 9 建立静态映射关系。

Switch(Config)#mac-address-table static address 00-01-22-22-22-22 vlan 1 interface ethernet 0/0/7

Switch(Config)#mac-address-table static address 00-01-33-33-33-33 vlan 1 interface ethernet 0/0/9

9.4 排错帮助

9.4.1监测和调试命令

9.4.1.1 show mac-address-table

命　令　：　show　mac-address-table [static|aging-time|blackhole] [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>]
功能：显示交换机当前的 MAC 地址表的内容。
参数：**static** 静态表项；**aging-time** 地址老化时间；**blackhole** 过滤表项；**<*mac-addr*>** 要显示的表项包含的MAC地址；**<*vlan-id*>** 要显示的表项包含的VLAN号；**<*interface-name*>** 要显示的表项包含的端口名称。
命令模式：特权用户配置模式
缺省情况：系统缺省不显示 MAC 地址表的内容。
使用指南：本命令可以分类显示各种 MAC 地址表项，也可以使用命令 **show mac-address-table** 显示当前交换机内所有的 MAC 地址表项。
举例：显示当前 MAC 地址表中的过滤表项。
Switch#show mac-address-table blackhole

9.4.2排错帮助

输入 show mac 命令时，某端口没有学习到该端口连接的设备的 MAC。可能的原因：

- 用于连接的以太网线损坏，更换以太网线；
- 交换机启动 SpanningTree，且端口处于 discarding 状态；或者端口刚连接上设备，Spanning Tree 还在计算中，等 Spanning Tree 计算完毕，端口就可以学习 MAC 地址了；
- 若不是上述的问题时，请查看是否是端口损坏，若是请找技术支持解决。

9.5 MAC 地址功能扩展

9.5.1MAC 地址绑定

9.5.1.1 MAC 地址绑定介绍

通常交换机支持动态学习 MAC 地址的功能，每个端口可以动态学习多个 MAC 地址，从而实现端口之间已知 MAC 地址数据流的转发。当 MAC 地址老化后，则进行广播处理。也就是说，交换机某接口上学习到某 MAC 地址后可以进行转发，如果将连线切换到另外一个接口上交换机将重新学习该 MAC 地址，从而在新切换的接口上实现数据转发。

但是，有些情况下为了安全和便于管理，需要将 MAC 地址与端口进行绑定，端口只允许已绑定 MAC 的数据流的转发。即，MAC 地址与端口绑定后，该 MAC 地址的数据流只能从绑定端口进入，其他没有与端口绑定的 MAC 地址的数据流不可以从该端口进入。

9.5.1.2 MAC 地址绑定配置

9.5.1.2.1 MAC 地址绑定配置任务序列

1. 使能端口的 MAC 地址绑定功能
2. 端口 MAC 地址的锁定
3. MAC 地址绑定的属性配置

命令	解释
接口配置模式	
switchport port-security **no switchport port-security**	使能端口 MAC 地址绑定功能；本命令的 no 操作为关闭端口 MAC 地址绑定功能。

1. 使能端口的 MAC 地址绑定功能

2. 端口 MAC 地址的锁定

命令	解释
接口配置模式	
switchport port-security lock **no switchport port-security lock**	锁定端口，当端口锁定之后，端口的 MAC 地址学习功能将被关闭；本命令的 no 操作恢复端口 MAC 地址学习功能。
switchport port-security convert	将端口学习到的动态安全 MAC 地址转化为静态安全 MAC 地址。
switchport port-security timeout <*value*> **no switchport port-security timeout**	打开端口锁定时器功能；本命令的 no 操作恢复默认值。
switchport port-security mac-address <*mac-address*> **no switchport port-security mac-address <*mac-address*>**	添加静态安全 MAC 地址；本命令的 no 操作为删除静态安全 MAC 地址。

命令	解释
接口配置模式	
switchport port-security maximum <*value*> **no switchport port-security maximum <*value*>**	设置交换机端口最大安全 MAC 地址数；本命令的 no 操作为恢复默认值。
switchport port-security violation {protect | shutdown} **no switchport port-security violation**	设置端口的违背模式；本命令的 no 操作为恢复默认值。
clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]	清除指定端口学习到的动态 MAC 地址。

3. MAC 地址绑定的属性配置

9.5.1.2.2 MAC 地址绑定配置命令

9.5.1.2.2.1 switchport port-security

命令：switchport port-security
no switchport port-security
功能：使能端口 MAC 地址绑定功能；本命令的 no 操作为关闭端口 MAC 地址绑定功能。
命令模式：接口配置模式
缺省情况：交换机端口不打开 MAC 地址绑定功能。
使用指南：MAC 地址绑定功能与 802.1x、Spanning Tree、端口汇聚功能存在互斥关系，因此如果要打开端口的 MAC 地址绑定功能，就必须关闭端口上的 802.1x、Spanning Tree、端口汇聚功能，且打开 MAC 地址绑定功能的端口不能是 Trunk 口。
举例：使能端口 1 的 MAC 地址绑定功能。
Switch(Config)#interface Ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#switchport port-security

9.5.1.2.2.2 switchport port-security convert

命令：switchport port-security convert
功能：将端口学习到的动态 MAC 地址转化为静态安全 MAC 地址。
命令模式：接口配置模式
使用指南：必须在安全端口锁定之后才能执行端口动态 MAC 地址转化命令。执行此命令之后，端口学习到的动态 MAC 地址将转化为静态安全 MAC 地址。该命令没有配置保留。
举例：将端口 1 的 MAC 地址转化为静态安全 MAC 地址。
Switch(Config)#interface Ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#switchport port-security convert

9.5.1.2.2.3 switchport port-security lock

命令：switchport port-security lock
no switchport port-security lock
功能：锁定端口。端口被锁定之后，端口的MAC地址学习功能将被关闭；本命令的no操作为恢复端口的MAC地址学习功能。
命令模式：接口配置模式
缺省情况：端口未锁定
使用指南：端口必须使能 MAC 地址绑定功能之后才能执行端口锁定命令。执行端口锁定命令之后，端口将关闭动态 MAC 学习功能。
举例：锁定端口 1。
Switch(Config)#interface Ethernet 0/0/1

Switch(Config-Ethernet0/0/1)#switchport
port-security lock

9.5.1.2.2.4 switchport port-security timeout

命令：**switchport port-security timeout <*value*>**
no switchport port-security timeout
功能：设置端口锁定的定时器；本命令的 no 操作为恢复缺省值。
参数：**<*value*>** 锁定时器时间间隔，取值范围为 0~300s。
命令模式：接口配置模式
缺省情况：端口未打开端口锁定的定时器。
使用指南：端口锁定定时器功能是一种动态 MAC 地址锁定功能，锁定定时器超时就执行 MAC 地址锁定操作及将动态 MAC 转换为安全 MAC 地址的操作。端口必须先开启 MAC 地址绑定功能后才能使用此命令。
举例：设置端口 1 的锁定时器为 30 秒。
Switch(Config)#interface Ethernet 0/0/1
Switch(Config-Ethernet0/0/1)# switchport port-security timeout 30

9.5.1.2.2.5 switchport port-security mac-address

命令：**switchport port-security mac-address <*mac-address*>**
no switchport port-security mac-address <*mac-address*>
功能：添加静态安全 MAC 地址；本命令的 no 操作为删除静态安全 MAC 地址。
命令模式：接口配置模式
参数：**<*mac-address*>**为添加/删除的 MAC 地址。
使用指南：端口必须使能 MAC 地址绑定功能之后才能添加端口静态安全 MAC 地址。
举例：添加 MAC 00-03-0F-FE-2E-D3 到端口 1。
Switch(Config)#interface Ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#switchport port-security mac-address 00-03-0F-FE-2E-D3

9.5.1.2.2.6 clear port-security dynamic

命令：**clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]**
功能：清除指定端口的动态 MAC 地址。
命令模式：特权用户配置模式
参数：**<*mac-addr*>**为 MAC 地址；**<*interface-id*>**为指定的端口号。
使用指南：必须在安全端口锁定之后之后才能执行指定端口的动态 MAC 清除操作。如果不指定端口、MAC 地址，则清除所有锁定的安全端口的动态 MAC；如果仅指定端口，不指定 MAC 地址，则清除指定端口的所有动态 MAC 地址。
举例：删除端口 1 动态 MAC。
Switch#clear port-security dynamic interface Ethernet 0/0/1

9.5.1.2.2.7 switchport port-security maximum

命令：switchport port-security maximum <*value*>
no switchport port-security maximum
功能：设置端口最大安全 MAC 地址数；本命令的 no 操作为恢复最大安全地址数为 1。
命令模式：接口配置模式
参数：<*value*> 端口静态安全 MAC 地址上限，取值范围 1~128。
缺省情况：端口最大安全 MAC 地址数为 1。
使用指南：端口必须使能 MAC 地址绑定功能之后才能设置端口安全 MAC 地址上限。如果端口静态安全 MAC 地址数大于设置的最大安全 MAC 地址数，则设置失败；必须删除端口的静态安全 MAC 地址，直到端口静态安全 MAC 地址数不大于设置的最大安全 MAC 地址数，设置才会成功。
举例：设置端口 1 安全 MAC 地址上限为 4。
Switch(Config)#interface Ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#switchport port-security maximum 4

9.5.1.2.2.8 switchport port-security violation

命令：switchport port-security violation {protect | shutdown}
no switchport port-security violation
功能：设置端口违背模式；本命令的 no 操作为恢复违背模式为 protect。
命令模式：接口配置模式
参数：protect 为保护模式；**shutdown** 为关闭模式。
缺省情况：端口违背模式为缺省为 **protect**。
使用指南：端口必须使能 MAC 地址绑定功能之后才能设置端口违背模式。如果端口违背模式设置为 **protect**，那么当端口安全 MAC 地址超过设置的端口安全 MAC 上限的时候，端口仅仅关闭动态 MAC 地址学习功能；如果端口违背模式设置为 **shutdown**，那么当端口安全 MAC 地址超过设置的端口安全 MAC 上限的时候，端口将被关闭，用户可以通过 **no shutdown** 命令手工打开该端口。
举例：设置端口 1 的违背模式为 shutdown。
Switch(Config)#interface Ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#switchport port-security violation shutdown

9.5.1.3 MAC 地址绑定排错帮助

9.5.1.3.1 MAC 地址绑定调试和监测命令

9.5.1.3.1.1 show port-security

命令：**show port-security**
功能：显示全局安全端口配置情况。
命令模式：特权用户配置模式
缺省情况：交换机不显示安全端口配置情况。
使用指南：本命令显示交换机当前已经配置为安全端口的端口信息 。
举例：

```
Switch#show port-security
Security Port        MaxSecurityAddr    CurrentAddr       Security Action
                         (count)              (count)
----------------------------------------------------------------
 Ethernet0/0/3              1                   1                Protect
 Ethernet0/0/4              10                  1                Protect
 Ethernet0/0/5              1                   0                Protect
----------------------------------------------------------------
Total Addresses in System :2
Max Addresses limit in System :128
```

显示信息	解释
Security Port	配置为安全端口的端口名
MaxSecurityAddr	安全端口设置的最大安全 MAC 地址数
CurrentAddr	安全端口当前安全 MAC 地址数
Security Action	端口设置的违背模式
Total Addresses in System	系统中当前安全 MAC 地址数
Max Addresses limit in System	系统中最大安全 MAC 地址数

9.5.1.3.1.2 show port-security interface

命令：**show port-security interface <*interface-id*>**
功能：显示安全端口配置情况。
命令模式：特权用户配置模式
参数：**<*interface-id*>** 指定的显示端口。
缺省情况：交换机不显示安全端口配置情况。
使用指南：本命令显示交换机安全端口的详细配置信息。
举例：

```
Switch#show port-security interface ethernet 0/0/1
Port Security :Enabled
Port status :Security Up
Violation mode :Protect
Maximum MAC Addresses :1
Total MAC Addresses :1
Configured MAC Addresses :1
Lock Timer is ShutDown
Mac-Learning function is : Opened
```

显示信息	解释
Port Security :	端口是否使能为安全端口
Port status :	端口安全状态
Violation mode :	端口设置的违背模式
Maximum MAC Addresses :	端口设置的安全 MAC 地址上限
Total MAC Addresses :	端口当前安全 MAC 地址数
Configured MAC Addresses :	端口静态配置的安全 MAC 地址数
Lock Timer	端口是否开启锁定的定时器（定时器时间）
Mac-Learning function	端口 MAC 地址学习功能是否打开

9.5.1.3.1.3 show port-security address

命令：show port-security address [interface <*interface-id*>]
功能：显示端口安全 MAC 地址。
命令模式：特权用户配置模式
参数：<*interface-id*> 指定的显示端口。
使用指南：本命令显示端口安全 MAC 地址信息，如果不指定端口则显示所有端口安全 MAC 地址。显示内容举例如下：

```
Switch#show port-security address interface ethernet 0/0/1
Security Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address         Type                Ports
 1      0000.0000.1111     SecureConfigured     Ethernet0/0/3
----------------------------------------------------------------------
Total Addresses :1
```

显示信息	解释
Vlan	安全 MAC 地址的 VLAN ID
Mac Address	安全 MAC 地址
Type	安全 MAC 地址类型
Ports	安全 MAC 地址所属端口
Total Addresses	系统中当前安全 MAC 地址数

9.5.1.3.2 MAC 地址绑定排错帮助

用户在端口使能 MAC 地址绑定功能的时候，有可能会遇到失败的情况。可能的原因及解决建议如下：

- 如果出现端口无法配置 MAC 地址绑定功能的情况，请检查交换机的端口是否运行了 Spanning-tree，802.1x，端口汇聚或者端口已经配置为 Trunk 端口。MAC 绑定在端口上与这些配置是互斥的，如果该端口要打开 MAC 地址绑定功能，就必须首先确认端口下的上述功能已经被关闭。

- 将安全地址设置为静态地址，然后删除，
  则该安全地址尽管存在，但已经不起作用。因此建议用户在 mac 绑定的端口不要设置静态地址。
- 用户有可能会遇到配置 MAC 地址绑定功能的端口连接的某些设备不能传输数据，请检查这些设备的 MAC 地址是否已经转换为安全 MAC，如果没有转换，即使学习到了这些设备的 MAC 地址，这些设备仍然不能传输数据，因为在配置 MAC 地址绑定功能的端口只有安全 MAC 才允许传输数据。

第10章VL
AN 配置

10.1 VLAN 介绍

VLAN（Virtual Local Area Network）即虚拟局域网，这项技术可以根据功能、应用或者管理的需要将局域网内部的设备逻辑地划分为一个个网段，从而形成一个个虚拟的工作组，并且不需要考虑设备的实际物理位置。IEEE 颁布了 IEEE802.1Q 协议以规定标准化 VLAN 的实现方案，本型号交换机的 VLAN 功能即按照 802.1Q 的标准实现。

VLAN 技术的特点在于可以动态的根据需要将一个大的局域网划分成许多不同的广播域：

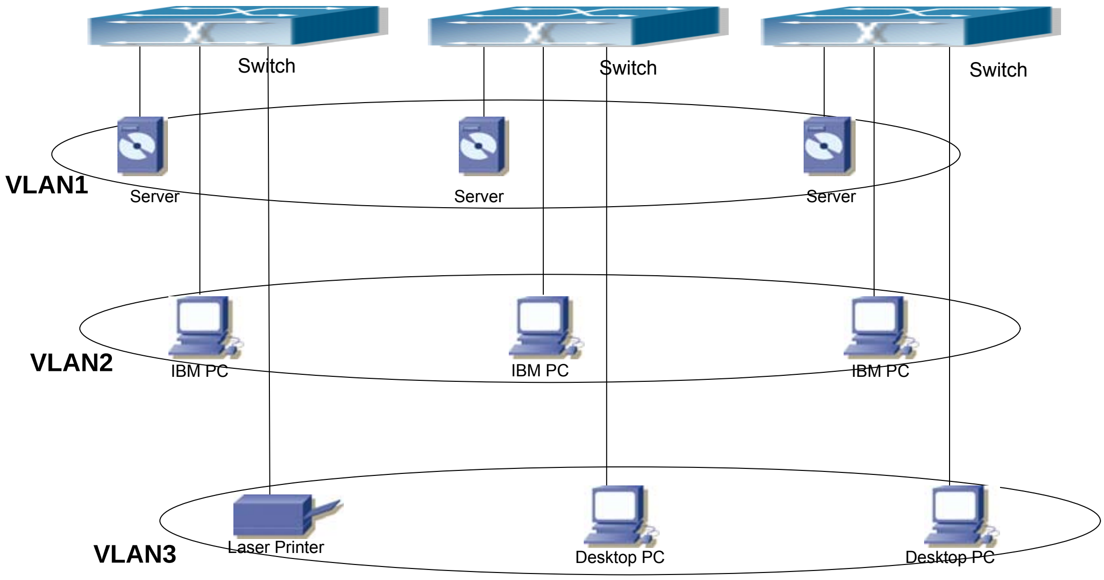


图 10-1 按照逻辑定义的 VLAN 网络

每个广播域即一个 VLAN，VLAN 和物理上的局域网有相同的属性，不同之处只在于 VLAN 是逻辑的而不是物理的划分，所以 VLAN 的划分不必根据实际的物理位置，而每个 VLAN 内部的广播、组播和单播流量都是与其它 VLAN 隔绝的。

基于 VLAN 的以上特性，VLAN 技术给我们带来以下的便利：

- 改善网络性能
- 节约网络资源
- 简化网络管理
- 降低网络成本
- 提高网络安全

在本型号交换机中，实现了 802.1Q 所定义的 VLAN 和 GVRP（GARP VLAN Registration Protocol），本章将对 VLAN 和 GVRP 的使用和配置进行详细的说明。

10.2 VLAN 配置

10.2.1 VLAN 的配置任务序列

1. 创建或删除 VLAN
2. 指定或删除 VLAN 名称
3. 为 VLAN 分配交换机端口
4. 设置交换机端口类型
5. 设置 Trunk 端口
6. 设置 Access 端口
7. 打开或关闭端口的 VLAN 入口规则
8. 配置 Private VLAN
9. 设置 Private VLAN 的绑定操作

1.创建或删除 VLAN

命令	解释
全局配置模式	
vlan <*vlan-id*> **no vlan <*vlan-id*>**	创建/删除 VLAN 或进入 VLAN 模式。

2.指定或删除 VLAN 名称

命令	解释
VLAN 配置模式	
name <*vlan-name*> **no name**	设置/删除 VLAN 名称。

3.为 VLAN 分配交换机端口

命令	解释
VLAN 配置模式	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	为 VLAN 分配交换机端口。

4.设置交换机端口类型

命令	解释
接口配置模式	
switchport mode {trunk|access}	设置当前端口为 Trunk 或 Access 端口。

5.设置 Trunk 端口

命令	解释
接口配置模式	
switchport trunk allowed vlan {<*vlan-list*>|all} **no switchport trunk allowed vlan <*vlan-list*>**	设置/删除 Trunk 端口允许通过的 VLAN。
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	设置/删除 Trunk 端口的 PVID。

6.设置 Access 端口

命令	解释
接口配置模式	
switchport access vlan <*vlan-id*> **no switchport access vlan**	将当前端口加入/退出到指定 VLAN。

7.打开或关闭 VLAN 的入口规则

命令	解释
全局配置模式	
vlan ingress enable **no vlan ingress enable**	打开及关闭 VLAN 的出口规则。

8．配置 Private VLAN

命令	解释
VLAN 配置模式	
private-vlan {primary|isolated|community} **no private-vlan**	将当前 VLAN 设置为 Private VLAN

9. 设置 Private VLAN 的绑定操作

命令	解释
VLAN 配置模式	
private-vlan association <*secondary-vlan-list*> **no private-vlan association**	设置/删除 Private VLAN 的绑定操作

10.2.2 VLAN 配置命令

10.2.2.1 vlan

命令：vlan <*vlan-id*>
no vlan <*vlan-id*>

功能：创建 VLAN 并且进入 VLAN 配置模式，在 VLAN 模式中，用户可以配置 VLAN 名称和为该 VLAN 分配交换机端口；本命令的 no 操作为删除指定的 VLAN。

参数：*<vlan-id>*为要创建/删除的 VLAN 的
VID，取值范围为 1~4094。
命令模式：全局配置模式
缺省情况：交换机缺省只有 VLAN1。
使用指南：VLAN1 为交换机的缺省 VLAN，用户不能配置和删除 VLAN1。允许配置 VLAN 的总共数量为 255 个。另需要提醒的是不能使用本命令删除通过 GVRP 学习到的动态 VLAN。
举例：创建 VLAN100，并且进入 VLAN100 的配置模式。
Switch(Config)#vlan 100
Switch(Config-Vlan100)#

10.2.2.2 name

命令：name *<vlan-name>*
no name
功能：为 VLAN 指定名称，VLAN 的名称是对该 VLAN 一个描述性字符串；本命令的 no 操作为删除 VLAN 的名称。
参数：*<vlan-name>*为指定的 vlan 名称字符串。
命令模式：VLAN 配置模式
缺省情况：VLAN 缺省 VLAN 名称为 vlanXXX，其中 XXX 为 VID。
使用指南：交换机提供为不同的 VLAN 指定名称的功能，有助于用户记忆 VLAN，方便管理。
举例：为 VLAN100 指定名称为 TestVlan。
Switch(Config-Vlan100)#name TestVlan

10.2.2.3 switchport access vlan

命令：switchport access vlan *<vlan-id>*
no switchport access vlan
功能：将当前 Access 端口加入到指定 VLAN；本命令 no 操作为将当前端口从 VLAN 里删除。
参数：*<vlan-id>*为当前端口要加入的 vlan VID，取值范围为 1~4094。
命令模式：接口配置模式
缺省情况：所有端口默认属于 VLAN1。
使用指南：只有属于 Access mode 的端口才能加入到指定的 VLAN 中，并且 Access 端口同时只能加入到一个 VLAN 里去。
举例：设置某 Access 端口加入 VLAN100。
Switch(Config)#interface ethernet 0/0/8
Switch(Config-ethernet0/0/8)#switchport mode access
Switch(Config-ethernet0/0/8)#switchport access vlan 100
Switch(Config-ethernet0/0/8)#exit

10.2.2.4 switchport interface

命令：switchport interface <*interface-list*>

no switchport interface <*interface-list*>

功能：给 VLAN 分配以太网端口的命令；本命令的 no 操作为删除指定 VLAN 内的一个或一组端口。

参数：<*interface-list*> 要添加或者删除的端口的列表，支持";" "-" ，如：ethernet 0/0/1;2;5 或 ethernet 0/0/1-6;8。

命令模式：VLAN 配置模式

缺省情况：新建立的 VLAN 缺省不包含任何端口。

使用指南：Access 端口为普通端口，可以加入 VLAN，但同时只允许加入一个 VLAN。

举例：为 VLAN100 分配百兆以太网端口 1，3，4-7，8。

Switch(Config-Vlan100)#switchport interface ethernet 0/0/1;3;4-7;8

10.2.2.5 switchport mode

命令：switchport mode {trunk|access}

功能：设置交换机的端口为 access 模式或者 trunk 模式。

参数：trunk 表示端口允许通过多个 VLAN 的流量；**access** 为端口只能属于一个 VLAN。

命令模式：接口配置模式

缺省情况：端口缺省为 Access 模式。

使用指南：工作在 trunk mode 下的端口称为 Trunk 端口，Trunk 端口可以通过多个 VLAN 的流量，通过 Trunk 端口之间的互联，可以实现不同交换机上的相同 VLAN 的互通；工作在 access mode 下的端口称为 Access 端口，Access 端口可以分配给一个 VLAN，并且同时只能分配给一个 VLAN。

注意在 Trunk 端口不允许 802.1X 认证。

举例：将端口 5 设置为 trunk 模式，端口 8 设置为 access 模式。

Switch(Config)#interface ethernet 0/0/5
Switch(Config-ethernet0/0/5)#switchport mode trunk
Switch(Config-ethernet0/0/5)#exit
Switch(Config)#interface ethernet 0/0/8
Switch(Config-ethernet0/0/8)#switchport mode access
Switch(Config-ethernet0/0/8)#exit

10.2.2.6 switchport trunk allowed vlan

命令：switchport trunk allowed vlan {<*vlan-list*>|all}

no switchport trunk allowed vlan

功能：设置 Trunk 端口允许通过 VLAN；本命令的 no 操作为恢复缺省情况。

参数：<*vlan-list*>为允许在该 Trunk 端口上通过的 VLAN 列表；**all** 关键字表示允许该 Trunk 端口通过所有 VLAN 的流量。

命令模式：接口配置模式

缺省情况：Trunk 端口缺省允许通过所有 VLAN。

使用指南：用户可以通过本命令设置哪些 VLAN 的流量通过 Trunk 端口，没有包含的 VLAN 流量则被禁止。

举例：设置 Trunk 端口允许通过 VLAN1，3，5-20 的流量。

Switch(Config)#interface ethernet 0/0/5
Switch(Config-ethernet0/0/5)#switchport mode trunk
Switch(Config-ethernet0/0/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-ethernet0/0/5)#exit

10.2.2.7 switchport trunk native vlan

命令：switchport trunk native vlan <*vlan-id*>
no switchport trunk native vlan
功能：设置 Trunk 端口的 PVID；本命令的 no 操作为恢复缺省值。
参数：<*vlan-id*>为 Trunk 端口的 PVID。
命令模式：接口配置模式
缺省情况：Trunk 端口默认的 PVID 为 1。
使用指南：在 802.1Q 中定义了 PVID 这个概念。Trunk 端口的 PVID 的作用是当一个 untagged 的帧进入 Trunk 端口，端口会对这个 untagged 帧打上带有本命令设置的 native PVID 的 tag 标记，用于 VLAN 的转发。
举例：设置某 Trunk 端口的 native vlan 为 100。
Switch(Config)#interface ethernet 0/0/5
Switch(Config-ethernet0/0/5)#switchport mode trunk
Switch(Config-ethernet0/0/5)#switchport trunk native vlan 100
Switch(Config-ethernet0/0/5)#exit

10.2.2.8 vlan ingress enable

命令：vlan ingress enable
no vlan ingress enable
功能：打开端口的 VLAN 入口规则；本命令的 no 操作为关闭入口准则。
命令模式：接口配置模式
缺省情况：系统缺省关闭端口的 VLAN 入口准则。
使用指南：当打开端口的 VLAN 入口规则，系统在接收数据时会检查源端口是否是该 VLAN 的成员端口，如果是则接受数据并转发到目的端口，否则丢弃该数据。
举例：打开端口的 VLAN 入口规则。
Switch(Config-Ethernet0/0/1)# vlan ingress enable

10.2.2.9 private-vlan

命令：private-vlan {primary|isolated|community}
no private-vlan
功能：将当前 VLAN 设置为 Private VLAN，该命令的 no 操作为取消 Private VLAN 设置。
参数：primary 将当前 VLAN 设置为 Primary VLAN，**isolated** 将当前 VLAN 设置为 Isolated VLAN，**community** 将当前 VLAN 设置为 Community VLAN。
命令模式：VLAN 配置模式
缺省情况：缺省没有 Private VLAN 配置。

使用指南：Private VLAN 分为三种：Primary VLAN，在 Primary VLAN 内的端口可以和关联到该 Primary VLAN 的 Isolated VLAN 和 Community VLAN 中的端口进行通信；Isolated VLAN，在 Isolated VLAN 内的端口之间是隔绝的，它们只可以和其相关联的 Primary VLAN 内的端口通信；Community VLAN，在 Community VLAN 内的端口相互之间可以通信，也也可以和其相关联的 Primary VLAN 内的端口通信；在 Isolated VLAN 内的端口和在 Community VLAN 内的端口之间不能通信。

只有不包含任何以太网端口的VLAN才能被设置为Private VLAN；只有设置了关联关系的Private VLAN才能将Access类型的以太网端口设置为成员端口；普通VLAN若被设置成Private VLAN后，会自动将所属以太网端口清空。

另外注意 GVRP 不传播 Private VLAN 的信息。

举例：将VLAN100、200、300设置为private vlan，类型分别为primary、Isolated、Community。

Switch(Config)#vlan 100
Switch(Config-Vlan100)#private-vlan primary
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
Switch(Config-Vlan200)#exit
Switch(Config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Switch(Config-Vlan300)#exit

10.2.2.10 private-vlan association

命令：private-vlan association <*secondary-vlan-list*>
no private-vlan association

功能：设置 Private VLAN 的绑定操作，该命令的 no 操作为取消 Private VLAN 绑定。

参数： **<*secondary-vlan-list*>** 为与指定 Primary VLAN 相关关联的 Secondary VLAN 列表，Secondary VLAN 包括 Isolated VLAN 和 Community VLAN 两种，支持";"连接多个 Secondary VLAN。

命令模式：VLAN 配置模式

缺省情况：缺省没有 Private VLAN 绑定。

使用指南：只有Primary类型的VLAN才能设置Private VLAN关联关系；被关联到Primary VLAN上的Secondary VLANs内的各个端口可以和关联的Primary VLAN内的各个端口进行通信。

在设置 Private VLAN 关联前，三种类型的 Private VLAN 都没有以太网端口的成员端口；存在 Private VLAN 关联关系的 Primary VLAN 不能被删除；被解除关联关系的 Private VLANs 会自动将所属成员端口清空。

举例：将Isolated VLAN200、Community VLAN300关联到Primary VLAN100上。

Switch(Config-Vlan100)#private-vlan association 200;300

10.2.3 VLAN 典型应用

案例

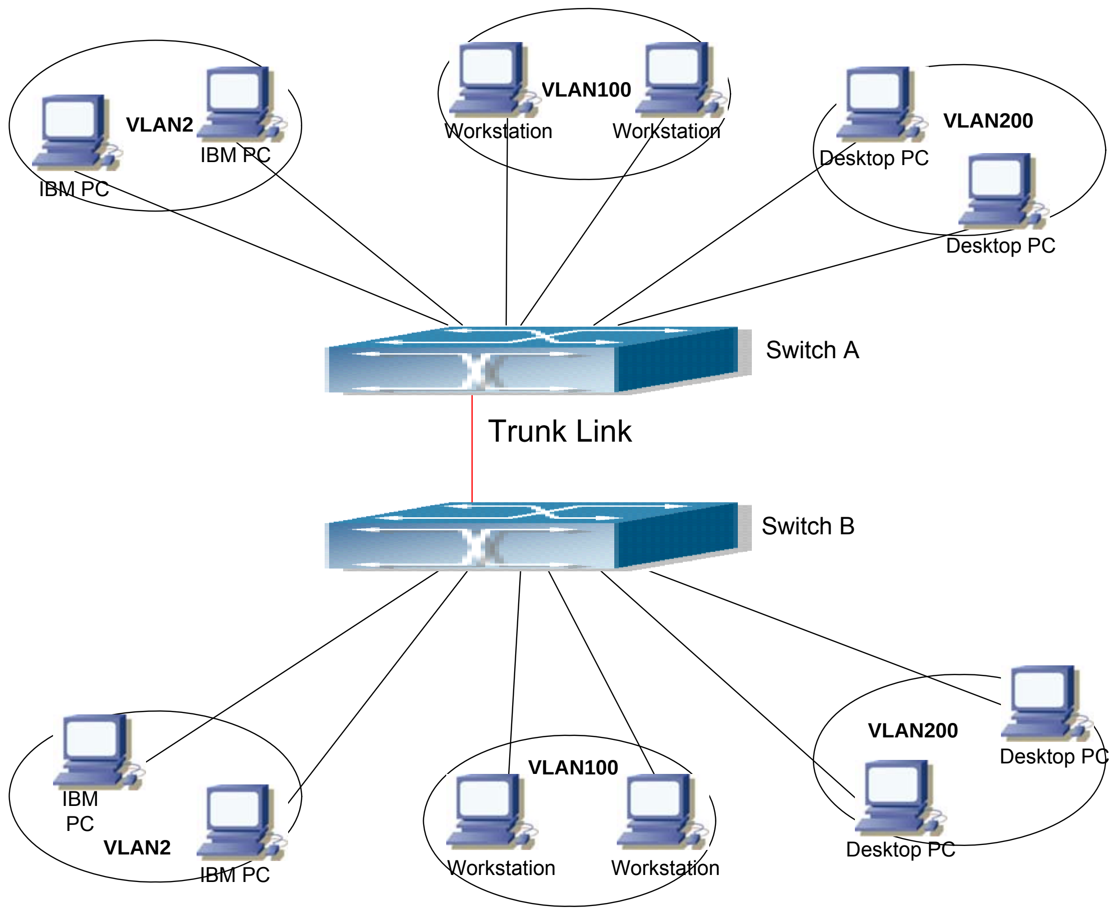


图 10-2 VLAN 典型应用拓扑图

由于局域网安全和应用的需要，需要将现有的整个局域网划分为 3 个 VLAN：VLAN2、VLAN100 和 VLAN200，并且要求这三个 VLAN 跨越两个地域 A 和 B，现在两处分别放置一台交换机，因此 VLAN 流量只要可以在交换机间传输，就可以满足跨地域的要求。

配置项目	配置说明
VLAN2	A 地、B 地交换机 2～8 号端口
VLAN100	A 地、B 地交换机 9～15 端口
VLAN200	A 地、B 地交换机 16～22 端口
Trunk port	A 地、B 地交换机的 23 号端口

将两台交换机的 Trunk port 相连，成为 Trunk link，用于承载跨交换机的 vlan 流量；将各种网络设备连接到交换机的各个 VLAN 的端口上，就归属到相应的 VLAN 之中。
在本例中，1 号和 24 号端口空闲，可以做为管理端口或其它用途。

配置步骤如下：
A 交换机:
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 0/0/2-8

Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 0/0/9-15
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 0/0/16-22
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 0/0/23
Switch(Config-Ethernet0/0/23)#switchport mode trunk
Switch(Config-Ethernet0/0/23)#exit
Switch(Config)#

B 交换机:

Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 0/0/2-8
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 0/0/9-15
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 0/0/16-22
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 0/0/23
Switch(Config-Ethernet0/0/23)#switchport mode trunk
Switch(Config-Ethernet0/0/23)#exit

10.3 端口隔离配置

private-vlan 中的 IsolateVlan 虽然可以达到端口隔离的效果，但如下的端口隔离需求 private-vlan 无法实现。

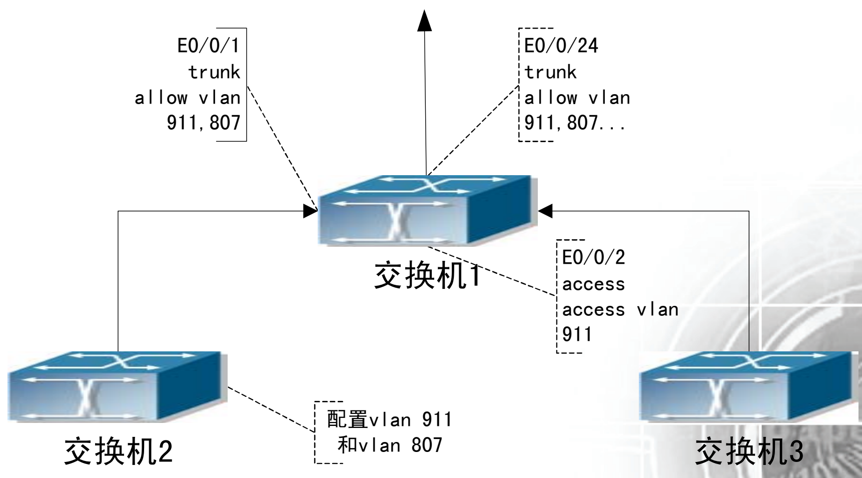


图 10-3 端口隔离

各个交换机的拓扑和配置如上图所示，要
求在交换机 1 上配置端口隔离后，交换机 1 的 e0/0/1 和 e0/0/2 不通，但 e0/0/1 和 e0/0/2 都可以和上联口 e0/0/24 通。即，所有下行端口之间不能互通，但下行端口可以和指定的上行端口互通。上行端口可以和所有端口互通。

神州数码交换机支持的端口隔离功能，可以实现以上需求。注：端口隔离功能无法跨堆叠使用。

10.3.1 端口隔离配置任务序列

1.设置上行端口

命令	解释
全局配置模式	
isolate-port allowed {[ethernet] <*InterfaceList*>}[deny-scheme|permit-scheme] **no isolate-port allowed [{[ethernet] <*InterfaceList*>}]**	设置或取消端口隔离功能，开启时要指定上行端口列表。可以反复调用此命令以分别设定或取消各个上行端口。

10.3.2 端口隔离配置命令

命令：**isolate-port allowed{[ethernet]<*InterfaceList*>}[deny-scheme|permit-scheme]**
no isolate-port allowed [{[ethernet] <*InterfaceList*>}]

功能：设置或取消端口隔离功能，开启时要指定上行端口列表。可以反复调用此命令以分别设定或取消各个上行端口。

参数：**<*InterfaceList*>**：上行端口列表，支持'-'和';'

<*deny-scheme*>：以deny-scheme模式进行端口隔离，上行口越多，耗费的硬件资源越少。

<*permit-scheme*>：以permit-scheme模式进行端口隔离，上行口越多，耗费的硬件资源越多。

命令模式：全局配置模式

缺省情况：用deny-scheme模式

使用指南:

1. 只要有上行端口，端口隔离功能就开启，即除了和上行端口可以互通以外，其余端口（当作下行端口）无法互通。
2. 当删除了所有上行端口后，端口隔离功能自动关闭，即所有端口可以互通。
3. 端口隔离目前只隔离IP包，因为如果全部隔离的话，ARP包将无法串过交换机。
4. 配置命令时操作硬件可能比较慢，最长可能会用2～3秒。

举例：以deny-scheme模式设置接口ethernet 0/0/1和ethernet 0/0/2为上行口，其余口为下行口进行端口隔离。

SWITCH(Config)#isolate-port allowed e0/0/1;0/0/2

10.4 GVRP 配置

GARP（Generic Attribute Registration Protocol），通用属性注册协议。GARP可以在交换网内的交换机成员之间动态分发传播注册某种属性信息，而这种属性可以是VLAN信息，也可以是组播MAC地址或者其它各种信息。实际上，GARP协议可以承载多种交换机需要传播的属性特征，而在GARP的基础上，定义了各种GARP应用，称为GARP应用实体，GVRP就是其中一种。

GVRP（GARP VLAN Registration Protocol），GARP VLAN 注册协议。GVRP 是基于 GARP 的工作机制的一种应用，负责维护交换机的 VLAN 动态注册信息，并且传播这些注册信息给其它的交换机。支持 GVRP 的交换机可以接受来自其它交换机的 VLAN 动态注册信息，并且根据这些信息更新本地的 VLAN 注册信息；支持 GVRP 的交换机也可以将本机的 VLAN 注册信息向其它交换机传播，GVRP 传播的 VLAN 注册信息即包括本地手工配置的静态信息，也包括从其它交换机学来的动态信息，这样，通过 VLAN 注册信息的传播，使得所有支持 GVRP 的交换机 VLAN 信息统一。

10.4.1 GVRP 配置任务序列

1. 配置GARP定时器参数
2. 开启GVRP功能

1.配置 GARP 定时器参数

命令	解释
接口配置模式	
garp timer join <*timer-value*> **no garp timer join** **garp timer leave <*timer-value*>** **no garp timer leave** **garp timer hold <*timer-value*>** **no garp timer hold**	配置 GARP 的 hold、join 和 leave 定时器。
全局配置模式	
garp timer leave all <*timer-value*> **no garp timer leave all**	配置 GARP 的 leave all 定时器。

2.开启 GVRP 功能

命令	解释
接口配置模式	
gvrp **no gvrp**	启动当前端口 GVRP 功能。
全局配置模式	
gvrp **no gvrp**	启动交换机 GVRP 功能。

10.4.2 GVRP 命令介绍

10.4.2.1 garp timer join

命令：**garp timer join <*timer-value*>**

no garp timer join

功能：配置 GARP 的 join 定时器的值；本命令的 no 操作为恢复定时器缺省值。

参数：**<*timer-value*>**为 join 定时器的值，取值范围为 100~327650ms。

命令模式：接口配置模式

缺省情况：join 定时器的缺省值为 200ms。

使用指南：GARP 应用实体在 join timer 超时之后，将发送 join 消息，其它 GARP 应用实体接收 join 消息后会注册该 GARP 应用实体的信息。用户配置 garp timers 的时候，必须满足如下关系：2*jointime < leavetime < leavealltime。

举例：设置端口 10 的 GARP join timer 值为 1000ms。

Switch(Config-Ethernet0/0/10)#garp timer join 1000

10.4.2.2 garp timer leave

命令：**garp timer leave <*timer-value*>**

no garp timer leave

功能：配置 GARP 的 leave 定时器的值；本命令的 no 操作为恢复定时器缺省值。

参数：**<*timer-value*>**为 leave 定时器的值，取值范围为 100~327650ms。

命令模式：接口配置模式

缺省情况：leave 定时器的缺省值为 600ms。

使用指南：GARP 应用实体在希望注销某属性信息的时候，将发送 leave 消息，收到该消息的 GARP 应用实体启动 leave 定时器，在 leave 定时器超时之前，如果没有再次受到 join 信息，则注销该属性信息。用户配置 garp timers 的时候，必须满足如下关系：2*jointime < leavetime < leavealltime。

举例：设置端口 0/0/10 的 GARP leave timer 值为 3000ms。

Switch(Config-Ethernet0/0/10)#garp timer leave 3000

10.4.2.3 garp timer hold

命令：**garp timer hold <*timer-value*>**

no garp timer hold

功能：配置 GARP 的 hold 定时器的值；本命令的 no 操作为恢复定时器缺省值。

参数：**<*timer-value*>**为 GARP hold 定时器的值，取值范围为 100~327650ms。

命令模式：接口配置模式

缺省情况：hold 定时器的缺省值为 100ms。

使用指南：GARP 应用实体在收到 join 消息时，不会马上向外发送 join 消息，而是启动 hold 定时器，hold 定时器超时后，把 hold 时间内收到的所有 join 消息，在一个 GVRP 帧里发送

出去，从而有效的减少协议消息流量。

举例：设置端口 0/0/10 的 GARP hold timer 值为 500ms。

Switch(Config-Ethernet0/0/10)#garp timer hold 500

10.4.2.4 garp timer leaveall

命令：garp timer leaveall <*timer-value*>

no garp timer leaveall

功能：配置 GARP 的 leaveall 定时器的值；本命令的 no 操作为恢复定时器缺省值。

参数：<*timer-value*>为 GARP leaveall timer 的值，取值范围为 100~327650ms。

命令模式：全局配置模式

缺省情况：leaveall 定时器缺省值为 10000ms。

使用指南： GARP 应用实体启动后，同时启动 leaveall 定时器，在 leaveall 定时器超时后，GARP 应用实体将向外发送 leaveall 消息，其它实体将注销该实体的一切属性信息，同时将 leaveall 定时器归零，启动新一轮循环。用户配置 garp timers 的时候，必须满足如下关系：2*jointime < leavetime < leavealltime。

举例：设置交换机的 GARP leaveall 定时器值为 50000ms。

Switch(Config)#garp timer leaveall 50000

10.4.2.5 gvrp

命令：gvrp

no gvrp

功能：启动交换机或者当前 Trunk 端口的 GVRP 功能；本命令的 no 操作为关闭全局或端口的 GVRP 功能。

命令模式：接口配置模式和全局配置模式

缺省情况：交换机缺省关闭 GVRP 功能。

使用指南：开启全局的 GVRP 功能后，才能开启端口的 GVRP。全局的 GVRP 关闭后，端口 GVRP 配置失效。注意 GVRP 只能在 Trunk 端口上开启。

举例：开启全局和 Trunk 端口 10 的 GVRP 功能。

Switch(Config)#gvrp

Switch(Config)#interface ethernet 0/0/10

Switch(Config-Ethernet0/0/10)#gvrp

Switch(Config)#exit

10.4.3 GVRP 典型应用

案例

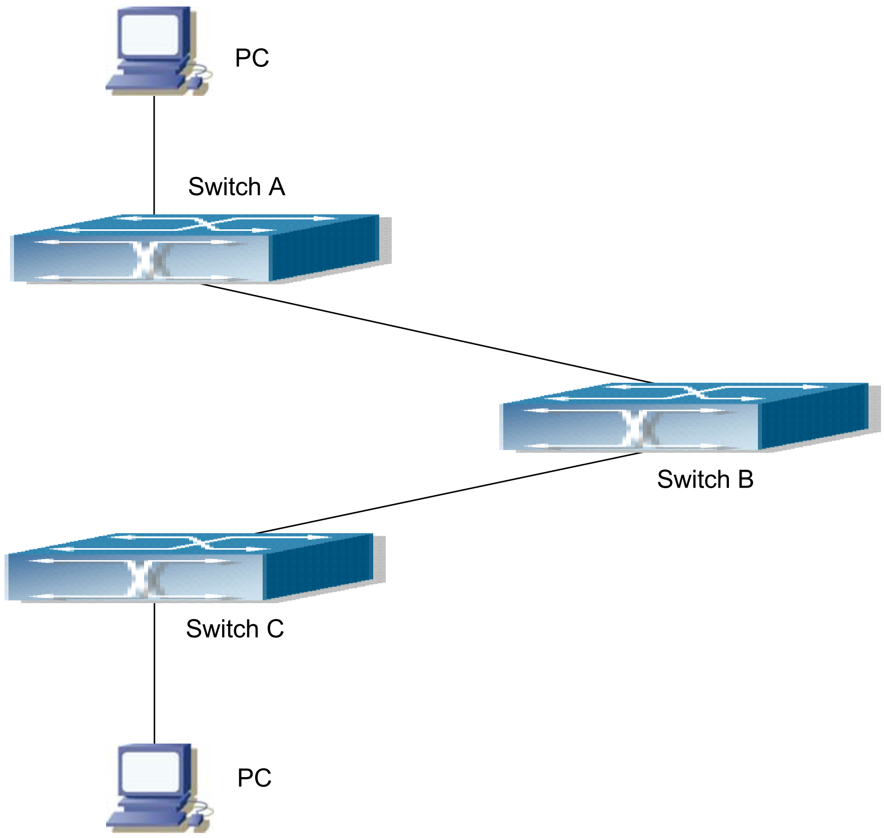


图 10-4 GVRP 典型应用拓扑图

为了实现交换机之间 VLAN 信息的动态注册和更新，需要在交换机上配置 GVRP 协议。在交换机 A、B 和 C 上配置 GVRP，使得交换机 B 学习到动态 VLAN100，这样，分别连接到交换机 A 和 C 的 VLAN100 上的两台工作站就可以通过没有配置静态 VLAN100 的交换机 B 互相通信。

配置项目	配置说明
VLAN100	交换机 A、C 的 12～16 端口
Trunk port	交换机 A、C 的 23 号端口，交换机 B 的 22、23 号端口
全局 GVRP	交换机 A、B、C
端口 GVRP	交换机 A、C 的 23 号端口，交换机 B 的 22、23 号端口

将两台工作站分别与交换机 A 和 B 的 VLAN100 的端口相连，将交换机 A 的 23 号端口与交换机 B 的 22 端口相连，交换机 B 的 23 号端口与交换机 C 的 23 号端口相连。

配置步骤如下：

Switch A:

Switch(Config)#gvrp

Switch(Config)#vlan 100

Switch(Config-Vlan100)#switchport interface ethernet 0/0/12-16

Switch(Config-Vlan100)#exit

Switch(Config)#interface Ethernet 0/0/23

Switch(Config-Ethernet0/0/23)#switchport
mode trunk
Switch(Config-Ethernet0/0/23)#gvrp
Switch(Config-Ethernet0/0/23)#exit

Switch B:
Switch(Config)#gvrp
Switch(Config)#interface ethernet 0/0/22
Switch(Config-Ethernet0/0/22)#switchport mode trunk
Switch(Config-Ethernet0/0/22)#gvrp
Switch(Config-Ethernet0/0/22)#exit
Switch(Config)#interface ethernet 0/0/23
Switch(Config-Ethernet0/0/23)#switchport mode trunk
Switch(Config-Ethernet0/0/23)#gvrp
Switch(Config-Ethernet0/0/23)#exit

Switch C:
Switch(Config)#gvrp
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 0/0/12-16
Switch(Config-Vlan100)#exit
Switch(Config)#interface ethernet 0/0/23
Switch(Config-Ethernet0/0/23)#switchport mode trunk
Switch(Config-Ethernet0/0/23)#gvrp
Switch(Config-Ethernet0/0/23)#exit

10.5 VLAN 排错帮助

10.5.1 监控和调试信息

10.5.1.1 show vlan

命令：show vlan [brief|internal usage|private-vlan] [id <*vlan-id*>] [name <vlan-name>]
功能：显示所有 VLAN 或者指定 VLAN 的详细状态信息。
参数：brief 简要信息；**internal usage** 显示内部 VLAN 的信息；**private-vlan** 显示 private vlan 信息；**<*vlan-id*>**为指定要显示状态信息的 VLAN 的 VLAN ID，取值范围 1~4094；**<*vlan-name*>**为指定要显示状态信息的 VLAN 的 VLAN 名，长度为 1~11。
命令模式：特权用户配置模式
使用指南：如果不指定**<*vlan-id*>**或**<*vlan-name*>**，则显示交换机所有 VLAN 的状态信息。
举例：显示 VLAN 1 的状态信息。
Switch#show vlan id 1

```
VLAN Name        Type      Status    Ports
---- ------------ ----------   --------- ---------------------------------------
1      default        Static     Active    Ethernet0/0/1             Ethernet0/0/2
                                      Ethernet0/0/3            Ethernet0/0/4
                                      Ethernet0/0/5            Ethernet0/0/6
                                      Ethernet0/0/7            Ethernet0/0/8
                                      Ethernet0/0/9            Ethernet0/0/10
                                      Ethernet0/0/11           Ethernet0/0/12
                                      Ethernet0/0/13           Ethernet0/0/14
                                      Ethernet0/0/15           Ethernet0/0/16
                                      Ethernet0/0/17           Ethernet0/0/18
                                      Ethernet0/0/19           Ethernet0/0/20
                                      Ethernet0/0/21           Ethernet0/0/22
                                      Ethernet0/0/23           Ethernet0/0/24

VLAN Type    MTU
----      -----      -----
1         ENET 1500
```

显示内容	解释
VLAN	VLAN 号；
Name	VLAN 名；
Type（第一个）	VLAN 的属性，是静态配置的还是动态学习到的。
Status	VLAN 的状态，为 active。
Ports	VLAN 内 Access 端口。
Type（第二个）	VLAN 的接口类型，为以太网类型。
MTU	最大传输数据单元，为 1500 字节

10.5.1.2 show garp

命令：**show garp [<*interface-name*>]**
功能：显示 GARP 的全局和端口信息。
参数：**<*interface-name*>**指定要显示的某个 Trunk 端口的端口名称。
命令模式：特权用户配置模式
使用指南：无。
举例：显示全局 GARP 信息。
switch#show garp

10.5.1.3 show gvrp

命令：**show gvrp [<*interface-name*>]**

功能：显示 GVRP 的全局和端口信息。
参数：***<interface-name>***指定要显示的某个 Trunk 端口的端口名称。
命令模式：特权用户配置模式
使用指南：无。
举例：显示全局 GVRP 信息。
switch#show gvrp
---------------- Gvrp Infomation ------------------
Gvrp status : enable
Gvrp Timers(milliseconds)
LeaveAll : 10000

10.5.1.4 debug gvrp

命令：**debug gvrp**
no debug gvrp
功能：打开交换机的 gvrp 的调试开关；本命令的 no 操作为关闭该调试开关。
命令模式：特权用户配置模式
缺省情况：缺省关闭交换机的 gvrp 的调试开关。
使用指南：用来打开交换机 gvrp 调试开关，可以显示交换机处理 gvrp 数据包信息。
举例：打开 gvrp 调试开关。
Switch#debug gvrp

10.5.2 VLAN 排错帮助

- Trunk 链路两端 Trunk 端口的 GARP 计数器设置必须相同，否则 GVRP 不能正常工作；
- 本型号交换机的 GVRP 功能不能和 RSTP 同时打开，如果要打开 GVRP 功能，请首先关闭端口的 RSTP 功能。

第11章MSTP 配置

11.1 MSTP 介绍

MSTP 是基于 STP 和 RSTP 的一种新的生成树协议。它运行在一个 Bridged-LAN 里的所有网桥上，负责为这个 Bridged-LAN（包括运行 MSTP、RSTP 和 STP 的网桥）计算出一个简单连通的树形活动拓扑(CIST)，为每个 MST 域（MSTP 域）计算出若干个各自独立的多重生成树实例(MSTI)。它应用 RSTP 的快速收敛特性，允许多个具有相同拓扑的 VLAN 映射到一个生成树实例上，而这个生成树拓扑同其它生成树实例相互独立。这种机制一方面用多重生成树实例为映射到它的 VLAN 的数据流量提供了独立的发送路径，实现不同实例间 VLAN 数据流量的负载分担；另一方面，若干个 VLAN 共享同一个拓扑实例（MSTI），同每个 VLAN 对应一个生成树（PVST）的实现方法相比，大大减少了每个网桥需要维持的生成树实例的数量，节约了 CPU 资源，降低了非业务带宽占有。

11.1.1 MSTP 域

由于多个 VLAN 可以映射到一个单一的生成树实例，IEEE 802.1s 委员会提出了 MST 域的概念，用来解决如何判断某个 VLAN 映射到哪个生成树实例的问题。

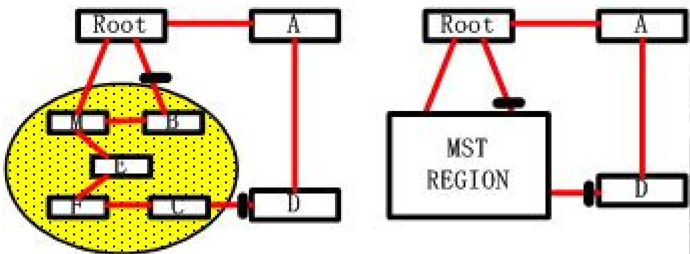
一个 MSTP 域由一个或若干个具有相同 MCID（MST Configuration Identification）的网桥和将网桥互连起来的局域网（域中的某个网桥是该局域网的指定桥，并且该局域网连接的网桥不是运行 STP 的网桥）组成。域中每个网桥维持相同的 MSTIs。

每个域中的网桥具有下述三个属性：

- 一个包含数字和字母的配置名字（Configuration Name）
- 一个配置修正级别（Revision Level）
- 网桥中 VLAN 向生产树实例映射的配置摘要（Configuration Digest）

以上三部分属性组成域的 MCID，只有这三部分属性完全相同，即 MCID 相同的网桥才被 MSTP 认为属于同一个 MST 域。

在整个 Bridged-LAN 的 CIST 中，MSTP 将 MST 域当做一个网桥对待，如下图所示：



对上图中的网络，如果网络中的网桥运行 STP 或 RSTP，应当 block（阻塞）网桥 M 和网桥 B 之间的一个端口。但是，如果图中黄颜色部分中的网桥运行 MSTP 并被配置在一

个 MST 域中，由于 MSTP 将该域当做一个网
桥对待，将会 block 网桥 B 上与根桥（Root）间的端口；同样，MSTP 会 block 网桥 D 上的某个端口。

11.1.1.1 MST 域内操作

在一个域内，IST 将域中所有的网桥连接起来。IST 在运行过程中，选出 CIST Regional Root 为它的根网桥，该网桥到 CIST Root 的路径代价和 BridgeID 最小。如果网络中只有一个域，该网桥就是整个网络的 CIST Root；如果 CIST Root 在该域外，则域边缘的某个网桥被选择为 CIST Regional Root。域中 CIST Regional Root 上的根端口是域中所有 MSTIs 的 Master Port。

当一个 MSTP 网桥初始化时，它发送 BPDU，声称自己是 CIST Regional Root，将到 CIST Root 和 CIST Regional Root 的路径代码设为 0。该网桥同时初始化所有 MSTIs，声称自己是所有 MSTIs 的根。如果该网桥收到更优的 CIST/MSTI 根信息（较小的路径代价，BridgeId 等），它就不再认为自己是 CIST 或相应 MSTI 的根。

在一个域中，只有 IST 发送和接收 BPDU。BPDU 中带有各个 MSTI 的信息。因为 MST BPDU 中包含了所有生成树实例的信息，大大减少了为支持多个生成树而需要处理的 BPDU 数量。

MST 域中的所有实例公用相同的协议定时器，但各个实例有各自独立的与拓扑相关的参数，如 Regional Root，根路径代价等。

11.1.1.2 MST 域间操作

当网络中存在多个 MST 域或 802.1D 网桥（运行 STP 的网桥）时，MSTP 通过 CST 维持域间或域同 802.1D 网桥间的连接。IST 将域中的网桥连接起来，作为一个虚拟的网桥同相邻的域或 802.1D 网桥连接。

MSTI 的作用范围仅局限于它所在的 MST 域中。一个域中的某个 MST 实例同其它域中的任何 MST 实例无关。域中的网桥通过边缘端口收到另外一个域发送来的 MST BPDU，它只处理数据中 CIST 的相关信息；而将其中的 MSTI 信息丢弃。

11.1.2 端口角色

MSTP 网桥为每一个运行 MSTP 的端口对应于每一个生成树分配一个端口角色。

- CIST的端口角色有：Root Port，Designated Port，Alternate Port和Backup Port。
- 每个MSTI的端口角色除了上述角色外，还增加了一个新的角色：Master Port。

CIST 和每个 MSTI 的 Root Port，Designated Port，Alternate Port 和 Backup Port 等角色的指定同 RSTP 对应的角色指定相同。

11.1.3 MSTP 流量分担的实现

在一个 MST 域中，通过将 VLAN 映射到不同的生成树实例，形成不同的拓扑。各个拓扑实例（包括 IST 和 MSTIs）间相互独立，可以在网桥中配置每个实例各自对应的参数（如

网桥优先级（Bridge Priority）、端口代价（Port Cost）等），为网桥和端口指定相应的角色，从而形成拓扑实例中 VLAN 数据流量对应的各自路径，实现 VLAN 流量的分担。具体配置可参考下面 MSTP 举例部分。

11.2 MSTP 配置

11.2.1 MSTP 配置任务序列

1. 启动 MSTP 并设置运行模式
2. 配置实例参数
3. 配置 MSTP 域参数
4. 配置 MSTP 的时间参数
5. 配置 MSTP 的快速迁移特性

1. 启动 MSTP 并设置运行模式

命令	解释
全局配置模式和端口配置模式	
spanning-tree **no spanning-tree**	启动和关闭 MSTP 协议。
全局配置模式	
spanning-tree mode {mstp|stp} **no spanning-tree mode**	设置 MSTP 的运行模式。
端口配置模式	
spanning-tree mcheck	强制端口迁移到 MSTP 模式下运行。

2. 配置实例参数

命令	解释
全局配置模式	
spanning-tree mst <*instance-id*> priority <*bridge-priority*> **no spanning-tree mst <*instance-id*> priority**	设置交换机指定实例的网桥优先级。
端口配置模式	
spanning-tree mst <*instance-id*> cost <*cost*> **no spanning-tree mst <*instance-id*> cost**	设置当前以太网端口指定实例的端口路径代价。
spanning-tree mst <*instance-id*> port-priority <*port-priority*> **no spanning-tree mst <*instance-id*> port-priority**	设置当前以太网端口指定实例的端口优先级。

3. 配置 MSTP 域参数

命令	解释
全局配置模式	
spanning-tree mst configuration **no spanning-tree mst configuration**	进入 MSTP 域配置模式；本命令的 no 操作为恢复交换机的 MSTP 域参数的缺省值。
MSTP 域配置模式	
instance <*instance-id*> vlan <*vlan-list*> **no instance <*instance-id*> [vlan <*vlan-list*>]**	创建 Instance 及配置 VLAN 与 Instance 的映射关系。
name <*name*> **no name**	配置 MSTP 域的名字。
revision-level <*level*> **no revision-level**	配置 MSTP 域的修正数值。
abort	退出 MSTP 域配置模式回到全局配置模式，不保存当前对 MSTP 域的配置。
exit	退出 MSTP 域配置模式回到全局配置模式，并保存当前对 MSTP 域的配置。

4. 配置 MSTP 的时间参数

命令	解释
全局配置模式	
spanning-tree forward-time <*time*> **no spanning-tree forward-time**	设置交换机转发延时的时间值。
spanning-tree hello-time <*time*> **no spanning-tree hello-time**	设置交换机发送 BPDU 报文的 Hello 时间值。
spanning-tree maxage <*time*> **no spanning-tree maxage**	设置交换机 BPDU 信息的最大老化时间值。
spanning-tree max-hop <*hop-count*> **no spanning-tree max-hop**	设置 BPDU 支持在 MSTP 域中传输的最大跳数。

5. 配置 MSTP 的快速迁移特性

命令	解释
端口配置模式	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	设置端口的链路类型。
spanning-tree portfast **no spanning-tree portfast**	设置和取消端口为边缘端口。

11.2.2 MSTP 配置命令介绍

11.2.2.1 abort

命令：abort
功能：放弃本次对 MSTP 域的配置，并且退出 MST 配置模式回到全局配置模式。
参数：无
命令模式：MSTP 域配置模式
使用指南：当使用本命令退出 MST 配置模式时，本次对 MSTP 域做的配置不生效，生效的仍然是前一次保留 MSTP 域配置。"Ctrl+z"命令相当于 abort 命令，即不保存配置直接退出。
举例：退出 MST 配置模式，并且不保留本次配置。
Switch(Config-Mstp-Region)#abort
Switch(Config)#

11.2.2.2 exit

命令：exit
功能：保存本次对 MSTP 域的配置，并且退出 MSTP 域配置模式回到全局配置模式。
参数：无
命令模式：MSTP 域配置模式
使用指南：当使用本命令退出 MST 配置模式时，本次对 MSTP 域做的配置即时生效。
举例：退出 MST 配置模式，并且保留本次配置。
Switch(Config-Mstp-Region)#exit
Switch(Config)#

11.2.2.3 instance vlan

命令：instance <*instance-id*> vlan <*vlan-list*>
no instance <*instance-id*> [vlan <*vlan-list*>]
功能：在 MSTP 域配置模式下，创建 Instance 及配置 VLAN 与 Instance 的映射关系或添加 VLAN 表项与指定 Instance 映射关系；本命令的 no 操作为删除指定的 Instance 或删除某些 VLAN 表项与指定 Instance 的映射关系。
参数：对于非 no 命令，**<*instance-id*>**为 Instance 号，取值范围为 0~48；对于 no 命令，**<*instance-id*>**为 Instance 号，取值范围为 1-48。**<*vlan-list*>**为连续的或不连续的 VLAN 号，支持表示连续的"-"符号和不连续的";"符号。
命令模式：MSTP 域配置模式
缺省情况：在没有创建任何 Instance 时，交换机只有 Instance 0，且 VLAN1~4094 均属于 Instance 0。
使用指南：本命令用于设置 VLAN 与 Instance 的映射关系，只有所有的映射关系都相同且其他 MSTP 域的参数也相同，交换机才能认为彼此是在相同的 MSTP 域中。在没有配置任何 Instance 时，所有的 VLAN 都属于 Instance 0。MSTP 最多支持 48 个 MSTI（除了 CIST 之外）。 可以把 CIST 理解为 MSTI0，其余实例为 MSTI1～48。具体个数依照产品规格而定，48 只是最大的规格值。

举例：配置 VLAN1-10;100-110 与 Instance 1
的映射关系；
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

11.2.2.4 name

命令：**name <*name*>**
no name
功能：在 MSTP 域配置模式下，配置 MSTP 域的名字；本命令的 no 操作为删除 MSTP 域的名字。
参数：**<*name*>**为 MSTP 域名字，取值范围不超过 32 字节的字符串。
命令模式：MSTP 域配置模式
缺省情况：缺省 MSTP 域为该交换机最小 VLAN 的 MAC。
使用指南：本命令用于设置 MSTP 域的名字，只有 MSTP 域的名字相同且其他 MSTP 域的参数也相同，交换机才能认为彼此是在相同的 MSTP 域中。
举例：配置 MSTP 域的名字为 DC-mstp-test。
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#name DC-mstp-test

11.2.2.5 revision-level

命令：**revision-level <*level*>**
no revision-level
功能：在 MST 配置模式下，配置用于计算 MST 配置标识的修正数值；本命令的 no 操作为恢复修正数值的缺省值 0。
参数：**<*level*>**为修正数值，取值范围为 0~65535。
命令模式：MSTP 域配置模式
缺省情况：缺省修正数值为 0。
使用指南：本命令用于设置计算 MST 配置标识时用到的修正数值，只有修正数值相同且其他 MSTP 域的参数也相同，交换机才能认为彼此是在相同的 MSTP 域中。
举例：配置修正数值为 2000。
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)# revision-level 2000

11.2.2.6 spanning-tree

命令：**spanning-tree**
no spanning-tree
功能：在交换机的全局配置模式和端口配置模式下分别启动 MSTP 协议的命令；本命令的 no 操作为关闭 MSTP 协议。
参数：无
命令模式：全局配置模式和端口配置模式
缺省情况：系统缺省不运行 MSTP 协议。

使用指南：如果在全局配置模式下启动了 MSTP 协议，所有的端口缺省都打开 MSTP 协议。**举例**：在全局模式打开 MSTP，并且在端口 0/0/2 模式关闭 MSTP。

Switch(Config)#spanning-tree
Switch(Config)#interface ethernet 0/0/2
Switch(Config-Ethernet0/0/2)#no spanning-tree

11.2.2.7 spanning-tree forward-time

命令：**spanning-tree forward-time <*time*>**
no spanning-tree forward-time
功能：设置交换机转发延时的时间值；本命令的 no 操作为恢复缺省值。
参数：***<time>***为转发延时的时间值，单位为秒，取值范围为 4~30。
命令模式：全局配置模式
缺省情况：转发延时缺省为 15 秒。
使用指南：当网络拓扑发生变换时，端口状态从阻塞状态转变到监听状态的这段延时称为转发延时。转发延时和 Hello 时间值、最大老化时间之间是有关联的，用户在配置 MSTP 时间参数时必须满足如下条件，否则会影响 MSTP 的正确工作：

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

举例：在全局模式配置 MSTP 转发延时时间为 20 秒。
Switch(Config)#spanning-tree forward-time 20

11.2.2.8 spanning-tree hello-time

命令：**spanning-tree hello-time <*time*>**
no spanning-tree hello-time
功能：设置交换机 Hello 时间值；本命令的 no 操作为恢复缺省值。
参数：***<time>***为 Hello time 的时间值，单位为秒，取值范围为 1~10。
命令模式：全局配置模式
缺省情况：Hello 时间缺省为 2 秒。
使用指南：交换机发送 BPDU 的时间间隔成为 Hello 时间。Hello 时间和转发延时、最大老化时间之间是有关联的，用户在配置 MSTP 时间参数时必须满足如下条件，否则会影响 MSTP 的正确工作：

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

举例：在全局模式配置 MSTP Hello 时间为 5 秒。
Switch(Config)#spanning-tree hello-time 5

11.2.2.9 spanning-tree link-type p2p

命令：**spanning-tree link-type p2p {auto|force-true|force-false}**
no spanning-tree link-type
功能：设置与当前端口相连的链路类型；本命令的 no 操作恢复当前端口的链路类型为自动

检测。
参数：auto 表示由系统自动检测链路类型，**force-true** 表示强制为点对点类型，**force-false** 表示强制为非点对点类型。
命令模式：端口配置模式
缺省情况：缺省情况下为 auto，MSTP 协议会自动检测端口相连的链路类型。
使用指南：当端口工作在全双工模式下，MSTP 协议会自动认为与该端口相连的链路类型为点对点类型；当端口工作在半双工模式下，MSTP 协议会自动认为与该端口相连的链路类型为共享型。
举例：强制交换机的端口 0/0/7-8 为点到点连接。
Switch(Config)#interface ethernet 0/0/7-8
Switch(Config-Port-Range)#spanning-tree link-type p2 force-true

11.2.2.10 spanning-tree maxage

命令：spanning-tree maxage <*time*>
no spanning-tree maxage
功能：设置交换机 BPDU 信息的最大老化时间值；本命令的 no 操作为恢复缺省值。
参数：<*time*>为最大老化时间值，单位为秒，取值范围为 6~40。
命令模式：全局配置模式
缺省情况：最大老化时间缺省为 20 秒。
使用指南：BPDU 的生命周期成为最大老化时间。最大老化时间和转发延时、Hello 时间之间是有关联的，用户在配置 MSTP 时间参数时必须满足如下条件，否则会影响 MSTP 的正确工作：
2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
举例：在全局模式配置 maxage 时间为 25 秒。
Switch(Config)#spanning-tree maxage 25

11.2.2.11 spanning-tree max-hop

命令：spanning-tree max-hop <*hop-count*>
no spanning-tree max-hop
功能：设置 BPDU 支持在 MSTP 域中传输的最大跳数；本命令的 no 操作为恢复缺省值。
参数：<*hop-count*>为最大跳数，取值范围为 1~40。
命令模式：全局配置模式
缺省情况：最大跳数缺省为 20。
在 MSTP 协议中不仅保留 Max-age 表示 BPDU 的生命周期，在 MSTP 域中还增加了 Max-hop 表示 BPDU 的生命周期，Max-hop 在网络中的传输呈递减状态。从 MSTI 的根网桥发出时 Max-hop 为最大值，BPDU 每被接收一次，该 BDPU 的 Max-hop 值就减少一跳，当交换机端口接收到 Max-hop 为 0 的 BPDU 时，该端口就会丢弃该 BPDU，并且将本端口作为指定端口发送 BDPU。
举例：设置最大跳数为 32。
Switch(Config)#spanning-tree max-hop 32

11.2.2.12 spanning-tree mcheck

命令：spanning-tree mcheck
功能：迫使交换机端口迁移到 MSTP 模式下运行。
参数：无
命令模式：以太网端口配置模式和 Port channel 接口模式。
缺省情况：端口运行在 MSTP 模式下。
使用指南：如果在与当前以太网端口相连的网段内存在运行 IEEE 802.1D STP 协议的网桥，该端口会迁移到 STP 兼容模式下运行。在网络比较稳定的情况下，虽然网段内运行 STP 协议的网桥被拆离，但与之相连的运行 MSTP 协议的交换机的端口仍然会运行在 STP 兼容模式下，此时可以通过该命令迫使其迁移到 MSTP 模式下运行。端口迁移到 MSTP 模式下运行后，如果再次收到新的 STP 报文，端口又会回到 STP 兼容模式下。

该命令必须在交换机运行在 IEEE802.1s MSTP 模式下时进行配置，如果交换机的协议运行模式被配置为 IEEE802.1D STP 模式，则该命令无效。
举例：强制端口 0/0/2 迁移到 MSTP 模式下运行。
Switch(Config-Ethernet0/0/2)#spanning-tree mcheck

11.2.2.13 spanning-tree mode

命令：spanning-tree mode {mstp|stp}
no spanning-tree mode
功能：设置交换机运行 Spanning Tree 的模式；本命令的 no 操作为恢复交换机缺省的模式。
参数：mstp 为设置交换机运行 IEEE802.1s 的 MSTP 模式；**stp** 为设置交换机运行 IEEE802.1D STP 模式。
命令模式：全局配置模式
缺省情况：交换机缺省运行 MSTP 模式。
使用指南：当交换机运行 IEEE802.1D STP 模式时，只能发送标准的 802.1D BPDU 帧和 TCN BPDU，对接收到的任何 MSTP BPDU 都将丢弃。
举例：设置交换机运行 STP 模式。
Switch(Config)#spanning-tree mode stp

11.2.2.14 spanning-tree mst configuration

命令：spanning-tree mst configuration
no spanning-tree mst configuration
功能：进入交换机的 MST 配置模式，在交换机的 MST 配置模式下，可配置交换机有关 MSTP 域的参数；本命令的 no 操作为恢复交换机的 MSTP 域参数的缺省值。
参数：无
命令模式：全局配置模式
缺省情况：用户在没有进入 MST 配置模式之前，MSTP 域的参数缺省如下：

MSTP 域参数	参数缺省值

Instance	只有实例 0 存在，且 VLAN1~4094 均映射在实例 0；
Name	取本交换机端口的最小 MAC；
Revision	0。

使用指南：无论交换机是否启动了 MSTP 协议，都可以进入 MSTP 域配置模式，并在配置后保存当前配置。当交换机运行 MSTP 模式时，系统会根据配置的 MSTP 域参数计算出本交换机的 MST 配置标识（MST Configuration Identifier），只有 MSTP 域配置标识相同的交换机才会认为是在同一个 MSTP 域中，且能进行 MSTI 的计算。

举例：进入交换机的 MST 配置模式。

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#

11.2.2.15 spanning-tree mst cost

命令：spanning-tree mst <*instance-id*> cost <*cost*>

no spanning-tree mst <instance-id> cost

功能：设置当前以太网端口指定实例的端口路径代价；本命令的 no 操作为恢复缺省值。

参数：<*instance-id*>为指定实例的实例 Id，取值范围为 1~48；**<*cost*>**为路径代价值，取值范围为 1~200,000,000。

命令模式：端口配置模式

缺省情况：缺省情况下，端口的路径代价与端口的带宽相关。

端口类型	缺省路径开销	建议取值范围
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000
10Gbps	2000	2000~20000

对汇聚端口，端口缺省路径代价如下：

端口类型	汇聚端口个数（在允许汇聚的个数范围内）	缺省路径开销
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

使用指南：通过配置端口路径代价可以控制该实例端口到根网桥的根路径代价，从而控制该实例根端口、指定端口等的选举。

举例：在端口 0/0/2 上设置实例 2 对应的 MSTP 端口路径代价为 3000000。

Switch(Config-Ethernet0/0/2)# spanning-tree mst 2 cost 3000000

11.2.2.16 spanning-tree mst port-priority

命令：spanning-tree mst <*instance-id*> port-priority <*port-priority*>

no spanning-tree mst <*instance-id*> port-priority

功能：设置当前端口指定实例的优先级值；本命令的 no 操作为恢复缺省端口的优先级值。

参数：<*instance-id*>为指定实例的实例 Id，取值范围为 1~48；**<*port-priority*>**为端口优先

级值，取值范围为 0~240 之间的 16 倍数，即
取值范围为 0、16、32、48…240。
命令模式：端口配置模式
缺省情况：端口缺省优先级值为 128。
使用指南：通过配置端口优先级可以控制指定实例的端口 ID，进而影响该实例的根端口、指定端口等选举。端口优先级值越小，优先级越高。
举例：在端口 0/0/2 设置实例 1 的端口优先级为 32。
Switch(Config)#interface ethernet 0/0/2
Switch(Config-ethernet0/0/2)#spanning-tree mst 1 port-priority 32

11.2.2.17 spanning-tree mst priority

命令：spanning-tree mst <*instance-id*> priority <*bridge-priority*>
no spanning-tree mst <*instance-id*> priority
功能：设置交换机指定实例的优先级；本命令的 no 操作为恢复交换机指定实例的缺省优先级值。
参数：<*instance-id*>为指定实例的实例 Id，取值范围为 0~48；**<*bridge-priority*>**为交换机的优先级，取值范围为 0~61440 之间的 4096 的倍数，即取值范围为 0、4096、8192…61440。
命令模式：全局配置模式
缺省情况：交换机缺省的优先级为 32768。
使用指南：通过配置交换机优先级可以改变指定实例的网桥 ID，进而用于该实例的根网桥、指定端口等选举。交换机优先级值越小，优先级越高。
举例：配置交换机实例 2 的优先级为 4096。
Switch(Config)#spanning-tree mst 2 priority 4096

11.2.2.18 spanning-tree portfast

命令：spanning-tree portfast
no spanning-tree portfast
功能：设置当前端口为边缘端口；本命令的 no 操作为设置当前端口为非边缘端口。
参数：无
命令模式：端口配置模式
缺省情况：所有端口在初始启动 MSTP 时均为非边缘端口。
使用指南：当端口被配置为边缘端口时，可以从 Discarding 状态立即转变到 Forwarding 状态，无须转发延时。一旦边缘端口接收到 BPDU 后，该端口就自动变化为非边缘端口。
举例：配置交换机的端口 0/0/5-6 为边缘端口。
Switch(Config)#interface ethernet 0/0/5-6
Switch(Config-Port-Range)#spanning-tree portfast

11.3 MSTP 举例

MSTP 典型应用案例如下：

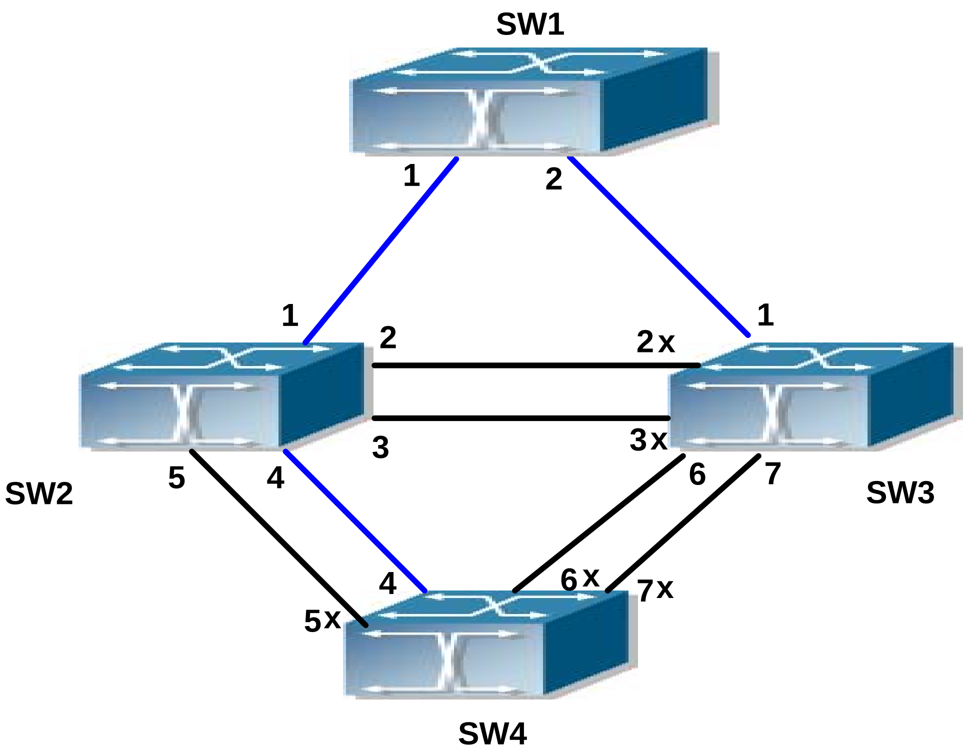


图 11-1 MSTP 典型配置举例

上图中，SW1-SW4 为神州数码交换机，各交换机之间的连线如图所示，运行 MSTP 协议。缺省条件下，各交换机运行在 MSTP 模式下，它们的网桥优先级、端口优先级、端口路径代价都为缺省值（都相等）。各交换机的缺省配置如下：

网桥名称		SW1	SW2	SW3	SW4
网桥 MAC 地址		…00-00-01	…00-00-02	…00-00-03	…00-00-04
网桥优先级		32768	32768	32768	32768
端口优先级	端口 0/0/1	128	128	128	
	端口 0/0/2	128	128	128	
	端口 0/0/3		128	128	
	端口 0/0/4		128		128
	端口 0/0/5		128		128
	端口 0/0/6			128	128
	端口 0/0/7			128	128
端口路径代价	端口 0/0/1	200000	200000	200000	
	端口 0/0/2	200000	200000	200000	
	端口 0/0/3		200000	200000	
	端口 0/0/4		200000		200000
	端口 0/0/5		200000		200000
	端口 0/0/6			200000	200000
	端口 0/0/7			200000	200000

在缺省情况下，MSTP 会自动建立起一个
以 SW1 为根网桥的拓扑（用蓝线标记），标记“×”的端口状态为 Discarding，其它端口状态为 Forwarding。

配置更改：
步骤一：配置端口到 vlan 的映射关系：

- 在交换机 SW2，SW3，SW4 上创建 vlan 20，30，40，50；
- 在交换机 SW2，SW3，SW4 配置端口 0/0/1-7 模式为 trunk。

步骤二：配置交换机 SW2，SW3，SW4 在同一个 MSTP 域内：

- 配置交换机 SW2，SW3，SW4 域名都为 digitalChina；
- 在交换机 SW2，SW3，SW4 上将 vlan 20 和 vlan 30 映射到实例 3 上；将 vlan 40 和 vlan 50 映射到实例 4 上。

步骤三：配置交换机 SW3 为实例 3 的根网桥；配置 SW4 交换机为实例 4 的跟网桥：

- 在交换机 SW3 上配置实例 3 对应的网桥优先级为 0；
- 在交换机 SW4 上配置实例 4 对应的网桥优先级为 0。

配置步骤如下：

交换机 **SW2:**

```
SW2(Config)#vlan 20
SW2(Config-Vlan20)#exit
SW2(Config)#vlan 30
SW2(Config-Vlan30)#exit
SW2(Config)#vlan 40
SW2(Config-Vlan40)#exit
SW2(Config)#vlan 50
SW2(Config-Vlan50)#exit
SW2(Config)#spanning-tree mst configuration
SW2(Config-Mstp-Region)#name digitalChina
SW2(Config-Mstp-Region)#instance 3 vlan 20;30
SW2(Config-Mstp-Region)#instance 4 vlan 40;50
SW2(Config-Mstp-Region)#exit
SW2(Config)#interface e0/0/1-7
SW2(Config-Port-Range)#switchport mode trunk
SW2(Config-Port-Range)#exit
SW2(Config)#spanning-tree
```

交换机 **SW3:**

```
SW3(Config)#vlan 20
SW3(Config-Vlan20)#exit
SW3(Config)#vlan 30
SW3(Config-Vlan30)#exit
SW3(Config)#vlan 40
SW3(Config-Vlan40)#exit
```

SW3(Config)#vlan 50
SW3(Config-Vlan50)#exit
SW3(Config)#spanning-tree mst configuration
SW3(Config-Mstp-Region)#name digitalChina
SW3(Config-Mstp-Region)#instance 3 vlan 20;30
SW3(Config-Mstp-Region)#instance 4 vlan 40;50
SW3(Config-Mstp-Region)#exit
SW3(Config)#interface e0/0/1-7
SW3(Config-Port-Range)#switchport mode trunk
SW3(Config-Port-Range)#exit
SW3(Config)#spanning-tree
SW3(Config)#spanning-tree mst 3 priority 0

交换机 **SW4:**
SW4(Config)#vlan 20
SW4(Config-Vlan20)#exit
SW4(Config)#vlan 30
SW4(Config-Vlan30)#exit
SW4(Config)#vlan 40
SW4(Config-Vlan40)#exit
SW4(Config)#vlan 50
SW4(Config-Vlan50)#exit
SW4(Config)#spanning-tree mst configuration
SW4(Config-Mstp-Region)#name digitalChina
SW4(Config-Mstp-Region)#instance 3 vlan 20;30
SW4(Config-Mstp-Region)#instance 4 vlan 40;50
SW4(Config-Mstp-Region)#exit
SW4(Config)#interface e0/0/1-7
SW4(Config-Port-Range)#switchport mode trunk
SW4(Config-Port-Range)#exit
SW4(Config)#spanning-tree
SW4(Config)#spanning-tree mst 4 priority 0

在上述配置之后，整个网络的实例 CIST（实例 0）以 SW1 为根网桥，在 SW2，SW3，SW4 所在的 MSTP 域内，实例 0 的域根（region root）是 SW2，实例 3 的域根是 SW3；实例 4 的域根是 SW4。vlan 20 和 vlan 30 的流量沿着实例 3 的拓扑的发送；vlan 40 和 vlan 50 的流量沿着实例 4 的拓扑的发送；其它 vlan 的流量沿实例 0 的拓扑发送。交换机 SW2 上的端口 0/0/1 是实例 3 和实例 4 的 Master Port。

MSTP 计算结果包括三个拓扑，实例 0，实例 3 和实例 4，分别如下所示（均用蓝线标记），标记“×”的端口状态为 Discarding，其它端口状态为 Forwarding。由于实例 3 和 4 只在 MSTP 域内有效，图中相关部分只显示其在 MSTP 域内的拓扑。

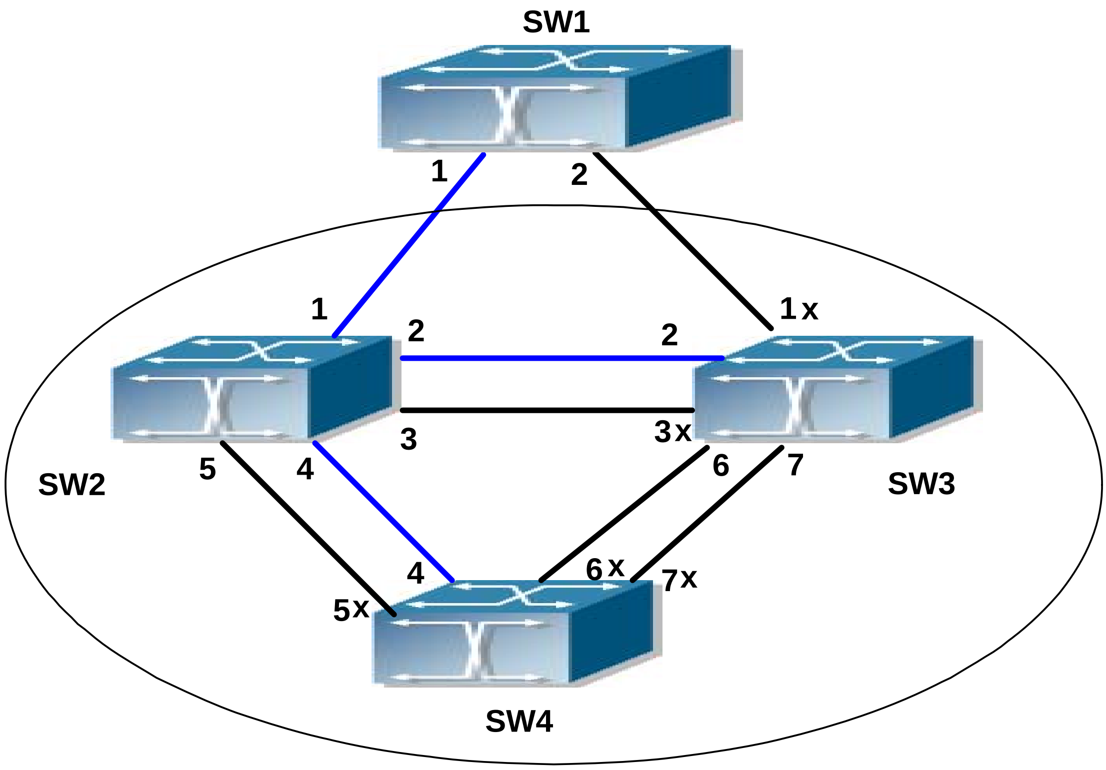


图 11-2　MSTP 变更后的实例 0 的拓扑

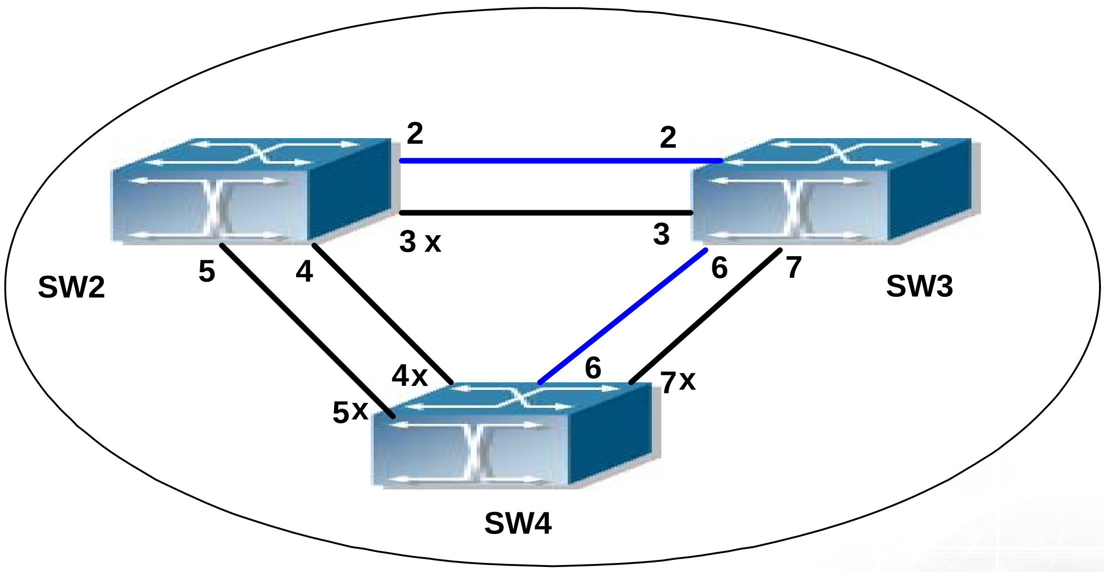


图 11-3　MSTP 变更后 MSTP 域内实例 3 的拓扑

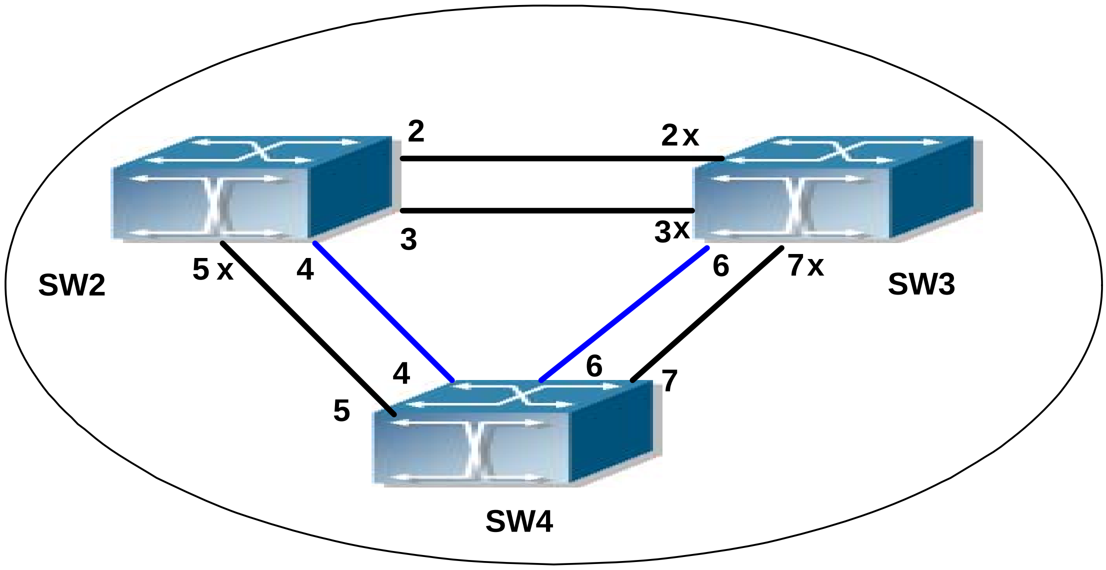


图 11-4 MSTP 变更后 MSTP 域内实例 4 的拓扑

11.4 MSTP 排错帮助

11.4.1 监测和调试命令

11.4.1.1 show spanning-tree

命令：show spanning-tree [mst [<*instance-id*>]] [interface <*interface-list*>] [detail]
功能：显示 MSTP 协议及各实例信息。
参数： **<*interface-list*>**为端口列表；**<*instance-id*>**为实例的值，范围为 0-48；**<*interface-list*>**为端口列表；**detail** 为显示详细的 spanning-tree 信息。
命令模式：特权模式
使用指南：通过 show spanning-tree 命令可以查看该网桥及各实例的 MSTP 信息，域配置信息以及端口的 MSTP 信息等。
举例：显示网桥 MSTP 信息，显示信息内容如下表所示。
SW1#sh spanning-tree

-- MSTP Bridge Config Info --

Standard : IEEE 802.1s
Bridge MAC : 00:03:0f:01:0e:30
Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 3

############################## Instance 0 ##############################
Self Bridge Id : 32768 - 00:03:0f:01:0e:30

```
Root Id              : 16384.00:03:0f:01:0f:52
Ext.RootPathCost : 200000
Region Root Id       : this switch
Int.RootPathCost : 0
Root Port ID         : 128.1
Current port list in Instance 0:
Ethernet0/0/1 Ethernet0/0/2 (Total 2)

 PortName        ID        ExtRPC     IntRPC   State Role       DsgBridge        DsgPort
-------------- -------- --------- --------- --- ---- ------------------ -------
 Ethernet0/0/1 128.001            0            0 FWD ROOT 16384.00030f010f52 128.007
 Ethernet0/0/2 128.002            0            0 BLK ALTR 16384.00030f010f52 128.011

############################ Instance 3 ############################
Self Bridge Id      : 0.00:03:0f:01:0e:30
Region Root Id       : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 3:
Ethernet0/0/1 Ethernet0/0/2 (Total 2)

  PortName        ID      IntRPC     State Role       DsgBridge        DsgPort
-------------- -------- --------- --- ---- ------------------ -------
 Ethernet0/0/1 128.001            0 FWD MSTR       0.00030f010e30 128.001
 Ethernet0/0/2 128.002            0 BLK ALTR       0.00030f010e30 128.002

############################ Instance 4 ############################
Self Bridge Id      : 32768.00:03:0f:01:0e:30
Region Root Id       : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 4:
Ethernet0/0/1 Ethernet0/0/2 (Total 2)

  PortName        ID      IntRPC     State Role       DsgBridge        DsgPort
-------------- -------- --------- --- ---- ------------------ -------
 Ethernet0/0/1 128.001            0 FWD MSTR 32768.00030f010e30 128.001
 Ethernet0/0/2 128.002            0 BLK ALTR 32768.00030f010e30 128.002
```

显示内容	解释
网桥信息	
Standard	STP 版本
Bridge MAC	代表本网桥的 MAC
Bridge Times	本网桥 Max Age，Hello Time 及 Forward Delay 的配置值

Force Version	当前运行 stp 协议的 Version 值
实例信息	
Self Bridge Id	该实例对应的本网桥优先级及 MAC
Root Id	该实例对应的根网桥优先级及 MAC
Ext.RootPathCost	网桥到整个网络总根的路径代价
Int.RootPathCost	网桥到该实例域根的路径代价
Root Port ID	网桥上该实例的根端口
该实例上 **MSTP** 协议生效的端口列表	
PortName	端口名字
ID	端口优先级及端口 index 索引值
ExtRPC	端口到整个网络总根的路径代价
IntRPC	端口到该实例域根的路径代价
State	该实例对应的端口状态
Role	该实例对应的端口角色
DsgBridge	该实例端口对应的上游指定网桥
DsgPort	该实例端口对应的上游指定端口

11.4.1.2 show mst configuration

命令：show spanning-tree mst config
功能：在特权模式下显示生效的 MSTP 域的参数配置情况。
参数：无
命令模式：特权配置模式
使用指南：在特权配置模式下，输入本命令可以查看 MSTP 域生效的当前参数，如 MSTP 域名、修正数值、VLAN 和 Instance 的映射情况。
举例：显示交换机的 MSTP 域的配置情况。
Switch #show spanning-tree mst config

```
Name        digitalChina
Revision    0
Instance    Vlans Mapped
----------------------------------
00          1-29, 31-39, 41-4094
03          30
04          40
----------------------------------
```

11.4.1.3 show mst-pending

命令：sh mst-pending
功能：在 MSTP 域配置模式下显示当前配置的未生效的 MSTP 域的参数配置情况。
命令模式：MSTP 域配置模式

参数：无

使用指南：在 MSTP 域配置模式下，输入本命令可以查看未生效的 MSTP 域当前参数，如 MSTP 域名字、修正数值、VLAN 和 Instance 的映射情况。

举例：显示交换机的 MSTP 域当前未生效的参数配置情况。

```
Switch (Config)#spanning-tree mst configuration
SW1(Config-Mstp-Region)#show mst-pending

Name        digitalChina
Revision     0
Instance     Vlans Mapped
----------------------------------
00            1-29, 31-39, 41-4093
03            30
04            40
05            4094
----------------------------------
SW1(Config-Mstp-Region)#
```

11.4.1.4 debug spanning-tree

命令：debug spanning-tree

no debug spanning-tree

功能：打开 MSTP 的调试信息；本命令的 no 操作为关闭 MSTP 调试信息。

参数：无

命令模式：特权模式

使用指南：该命令是 MSTP 庞大复杂 debug 功能的总开关，逐级打开需要 debug 的相应信息开关后再打开此总开关就能够输出 debug 打印信息了。各级 debug 开关的功能包括：查看 MSTP 协议运行中 bpdu 报文的发送接收、事件的处理、状态机、计时器等等。一般情况下，这些调试信息是给技术人员调试使用，用户不需要关注。

举例：打开端口 e0/0/1 接收 BPDU 报文的 debug 信息。

```
Switch#debug spanning-tree
Switch#debug spanning-tree bpdu rx interface e0/0/1
```

11.4.2 MSTP 排错帮助

- 如果想在交换机上运行 MSTP，首先必须在全局打开 MSTP 开关。在没有打开全局 MSTP 开关之前，打开端口的 MSTP 开关是不允许的。
- MSTP 定时器参数之间是有相关性的，错误配置可能导致交换机不能正常工作。各定时器之间的关联关系为：2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
  Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
- 用户在修改MSTP参数时，应该清楚所产生的各个拓扑。除了全局的基于网桥的参数配置外，其它的是基于各个实例的配置，在配置时一定要注意配置参数对应的实例是否正确。

☞ 神州数码交换机的端口MSTP功能与端口MAC绑定、802.1x和设置端口为路由端口功能互斥。当端口已经配置MAC绑定、802.1x或设置为路由端口时，无法在该端口启动MSTP功能。

第12章IG MP Snooping 配置

12.1 IGMP Snooping 介绍

IGMP（Internet Group Management Protocol）互联网组管理协议，用于实现IP的组播。IGMP被支持组播的网络设备（如路由器）用来进行主机资格查询，也被想加入某组播组的主机用来通知路由器接受某个组播地址的数据包，而这些都是通过IGMP消息交换来完成的。路由器首先利用一个可寻址到所有主机的组地址（即224.0.0.1）发送一条IGMP主机成员资格查寻（IGMP Host Membership Query）消息。若一个主机希望加入某组播组，它就利用该组播组的组地址回应一条IGMP主机成员资格报告（IGMP Host Membership Report）消息。

IGMP Snooping 即 IGMP 侦听。交换机通过 IGMP Snooping 来限制组播流量的泛滥，只把组播流量转发给与组播设备相连的端口。交换机侦听组播路由器和主机之间的 IGMP 消息，根据侦听结果维护组播转发表，而交换机根据组播转发表来决定组播包的转发。

神州数码交换机实现了 IGMP Snooping 功能，同时还提供交换机发送 Query 的功能，这样，用户可以用神州数码交换机实现 IP 组播。

12.2 IGMP Snooping 配置

12.2.1 IGMP Snooping 配置任务

1.启动 IGMP Snooping 功能
2.配置 IGMP Snooping
3.配置发送 IGMP Query

1.启动 IGMP Snooping 功能

命令	解释
全局配置模式	
ip igmp snooping **no ip igmp snooping**	启动 IGMP Snooping 功能。

2.配置 IGMP Snooping

命令	解释
全局配置模式	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	启动指定 VLAN 的 IGMP Snooping 功能。
ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*>	设置指定 VLAN 内的连接 M-router 的端口。

no ip igmp snooping vlan <*vlan-id*> mrouter	
ip igmp snooping vlan <*vlan-id*> immediate-leave **no ip igmp snooping vlan <*vlan-id*> immediate-leave**	设置指定VLAN的IGMP Snooping具有快速离开组播组功能。
ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*> interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*>**	配置静态的组播地址及加入的端口成员。

3.配置 IGMP 发送 Query

命令	解释
全局配置模式	
ip igmp snooping vlan <*vlan-id*> query **no ip igmp snooping vlan <*vlan-id*> query**	打开指定 VLAN 的 IGMP Snooping 发送 Query 功能。
ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*> **no ip igmp snooping vlan <*vlan-id*> query robustness**	设置指定 VLAN 的 IGMP Snooping Query 功能的活力参数。
ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*> **no ip igmp snooping vlan <*vlan-id*> query interval**	设置指定 VLAN 的 IGMP Snooping Query 功能的发送间隔。
ip igmp snooping vlan <*vlan-id*> query max-response <*time-value*>} **no ip igmp snooping vlan <*vlan-id*> query max-response**	设置指定 VLAN 的 IGMP Snooping Query 功能的最大响应时间。

12.2.2 IGMP Snooping 配置命令

12.2.2.1 ip igmp snooping

命令：**ip igmp snooping**
no ip igmp snooping
功能：打开交换机的 IGMP Snooping 功能；本命令的 no 操作为关闭 IGMP Snooping。
命令模式：全局配置模式
缺省情况：交换机缺省不启动 IGMP Snooping。
使用指南：启动交换机的 IGMP Snooping 功能，使交换机能够监视网络的组播流量，并且

决定哪些端口可以接收组播流量。
举例：在全局模式启动 IGMP snooping。
Switch(Config)#ip igmp snooping

12.2.2.2 ip igmp snooping vlan

命令：ip igmp snooping vlan <*vlan-id*>
no ip igmp snooping vlan <*vlan-id*>
功能：打开指定 VLAN 的 IGMP Snooping 功能；本命令的 no 操作为关闭指定 VLAN 的 IGMP Snooping 功能。
参数：<*vlan-id*>为 VLAN 号。
命令模式：全局配置模式
缺省情况：VLAN 缺省不打开 IGMP Snooping。
使用指南：必须先打开交换机的 IGMP Snooping 功能，才能打开指定 VLAN 的 IGMP Snooping 功能。本命令与命令 **ip igmp snooping vlan <*vlan-id*> query** 互斥，即在同一个 VLAN 中同时只能做 snooping 或者 query 中的一种功能。
举例：在全局配置模式下启动 VLAN 100 的 IGMP snooping 功能。
Switch(Config)#ip igmp snooping vlan 100

12.2.2.3 ip igmp snooping vlan mrouter

命令：ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*>
no ip igmp snooping vlan <*vlan-id*> mrouter
功能：在指定 VLAN 内配置静态组播路由端口；本命令的 no 操作为删除组播路由端口。
参数：<*vlan-id*>为指定的 VLAN 号；**<*interface –name*>**为指定组播路由端口号。
命令模式：全局配置模式
缺省情况：缺省 VLAN 内没有 M-Router 端口。
使用指南：在打开 IGMP Snooping 功能的 VLAN 内必须设置 M-Router 端口，否则 IGMP 数据包将被丢弃，导致不能在指定 VLAN 内进行 IGMP Snooping。
举例：指定 VLAN 100 的 M-Router 端口为 0/0/6 号端口。
Switch(Config)#ip igmp snooping vlan 100 mrouter interface eth 0/0/6

12.2.2.4 ip igmp snooping vlan static

命令：ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*> interface <*interface –name*>
no ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*>
功能：设置 IGMP snooping 静态组播组成员功能，该命令的 no 操作为取消该功能。
参数：<*vlan-id*> 指定 VLAN 号；**<*multicast-ip-addr*>** 组播 IP 地址；**<*interface-name*>** 组播组成员端口。
命令模式：全局配置模式
缺省情况：缺省没有静态组播组
使用指南：当加入的静态组播地址已经存在，并且是动态的地址，则静态的地址将覆盖动态

的。

举例：在 VLAN 100 新建一个静态组播地址 224.1.1.1，并且将 0/0/6 号端口加入该组。

Switch(Config)#ip igmp snooping vlan 100 static 224.1.1.1 interface eth0/0/6

将 VLAN 100 上的静态组播地址 224.1.1.1 删除

Switch(Config)#no ip igmp snooping vlan 100 static 224.1.1.1

12.2.2.5 ip igmp snooping vlan immediate-leave

命令：**ip igmp snooping vlan <*vlan-id*> immediate-leave**

no ip igmp snooping vlan <*vlan-id*> immediate-leave

功能：打开指定 VLAN 内 IGMP 协议的快速离开功能；本命令的 no 操作为关闭 IGMP 协议的快速离开功能。

参数：**<*vlan-id*>**为指定的 VLAN 号。

命令模式：全局配置模式

缺省情况：缺省关闭该功能。

使用指南：打开 IGMP 协议的快速离开功能，可以加速对端口离开组播组的处理。本命令只对 Snooping 功能有效，对 Query 功能无效。

举例：打开 VLAN 100 的 IGMP 快速离开功能。

Switch(Config)#ip igmp snooping vlan 100 immediate-leave

12.2.2.6 ip igmp snooping vlan query

命令：**ip igmp snooping vlan <*vlan-id*> query**

no ip igmp snooping vlan <*vlan-id*> query

功能：打开指定 VLAN 的 IGMP Query 功能；本命令的 no 操作为关闭 Query 功能。

参数：**<*vlan-id*>**为指定的 VALN 号。

命令模式：全局配置模式

缺省情况：缺省不打开 IGMP Query 功能。

使用指南：打开指定 VLAN 内的 IGMP Query 功能的前提是，首先交换机上配置有相应的 VLAN，并且启动了交换机的 IGMP Snooping。需要注意，本命令与命令 **ip igmp snooping vlan <*vlan-id*>**互斥，即在同一 VLAN 内同时只能做 Snooping 或者 Query 中的一种功能。

举例：打开 VLAN100 的 IGMP Query 功能。

Switch(Config)#ip igmp snooping vlan 100 query

12.2.2.7 ip igmp snooping vlan query robustness

命令：**ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*>**

no ip igmp snooping vlan <*vlan-id*> query robustness

功能：设置指定 VLAN 内的 IGMP Query 功能的活力参数；本命令的 no 操作为恢复默认值。

参数：**<*vlan-id*>**为指定的 VLAN 号；**<*robustness-variable*>**为活力参数，取值范围为 2~10。

命令模式：全局配置模式

缺省情况：活力参数的缺省值为 2。

使用指南：活力参数越大，表示网络环境越糟糕；活力参数越小，表示网络环境越大，用户

可以根据实际网络适当的设置活力参数。

举例：配置 VLAN100 的 IGMP Query 的活力参数为 3。

Switch(Config)#ip igmp snooping vlan 100 query robustness 3

12.2.2.8 ip igmp snooping vlan query interval

命令：ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*>

no ip igmp snooping vlan <*vlan-id*> query interval

功能：设置指定 VLAN 内的发送 IGMP Query 的时间间隔；本命令的 no 操作为恢复默认值。

参数：*<vlan-id>*为指定的 VLAN 号；***<interval-value>***为发送 Query 的时间间隔，取值范围为 10~65535。

命令模式：全局配置模式

缺省情况：缺省发送 Query 的时间间隔为 125 秒。

举例：配置 VLAN 100 发送 IGMP Query 的时间间隔为 60 秒。

Switch(Config)#ip igmp snooping vlan 100 query interval 60

12.2.2.9 ip igmp snooping vlan query max-response-time

命令：ip igmp snooping vlan <*vlan-id*> query max-response-time <*time-value*>

no ip igmp snooping vlan <*vlan-id*> query max-response-time

功能：设置指定 VLAN 内的 IGMP Query 的最大响应时间；本命令的 no 操作为恢复默认值。

参数：*<vlan-id>*为指定的 VLAN 号；***<time-value>***为指定最大 Query 响应时间，取值范围为 10~25。

命令模式：全局配置模式

缺省情况：最大 Query 响应时间的缺省值为 10 秒。

举例：配置 VLAN100 的 IGMP 最大 Query 响应时间为 12 秒。

Switch(Config)#ip igmp snooping vlan 100 query max-response-time 12

12.3 IGMP Snooping 举例

案例 1：IGMP Snooping 功能。

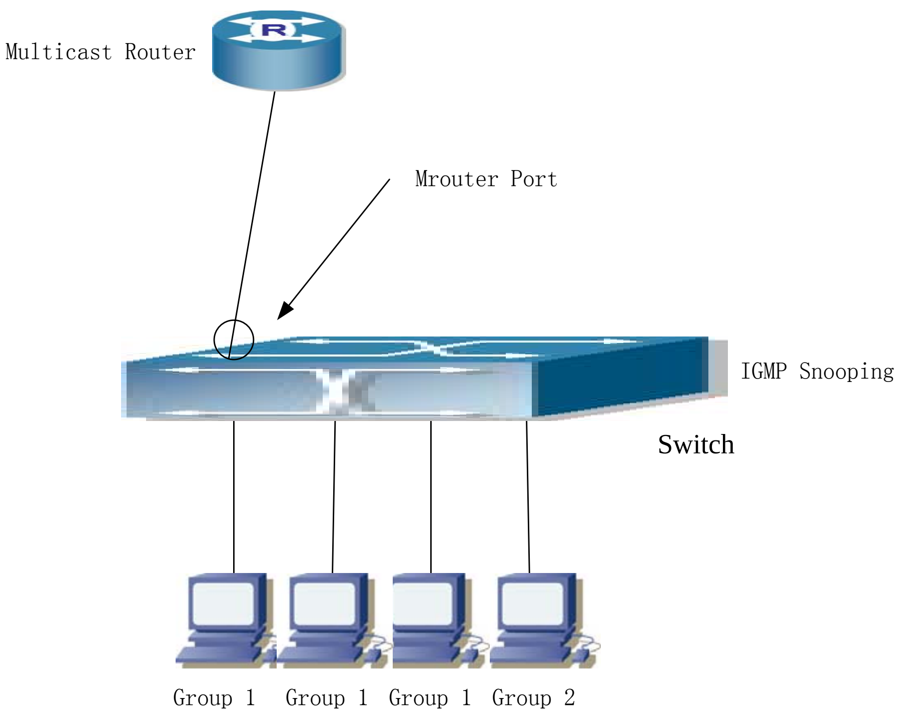


图 12-1 打开交换机 IGMP Snooping 功能图

如图所示，Switch 上配置 vlan 100 包含端口 1、2、6、10、20。四台主机分别连在端口 2、6、10、20 上，组播路由器连在端口 1 上。假设我们需要在 vlan 100 上做 igmp snooping。缺省情况下，交换机的全局 igmp snooping 功能和各 VLAN 上的 igmp snooping 功能都不打开。因此，需要打开全局下的 igmp snooping 功能，同时在 vlan 100 上打开 igmp snooping，还需要设置 vlan 100 的 mrouter 端口为 1 号端口。

配置步骤如下：

Switch #config
Switch (config)#ip igmp snooping
Switch (config)#ip igmp snooping vlan 100
Switch (config)#ip igmp snooping vlan 100 mrouter interface ethernet 0/0/1

组播配置：

假设组播服务器 Multicast Server 提供两个节目，分别使用组地址 Group1 和 Group2，四台主机上同时运行组播应用软件，连在端口 2、6、10 上的三台主机播放节目 1，连在端口 20 上的主机播放节目 2。

IGMP snooping 侦听结果：

vlan 100 上 igmp snooping 建立的组播表显示：端口 1、2、6、10 在组 Group1 中，端口 1、20 在组 Group2 中。

四台主机都能正常地收到自己感兴趣的节目，端口 2、6、10 不会收到节目 2 的流量，端口 20 不会收到节目 1 的流量。

案例 2：**IGMP Query**

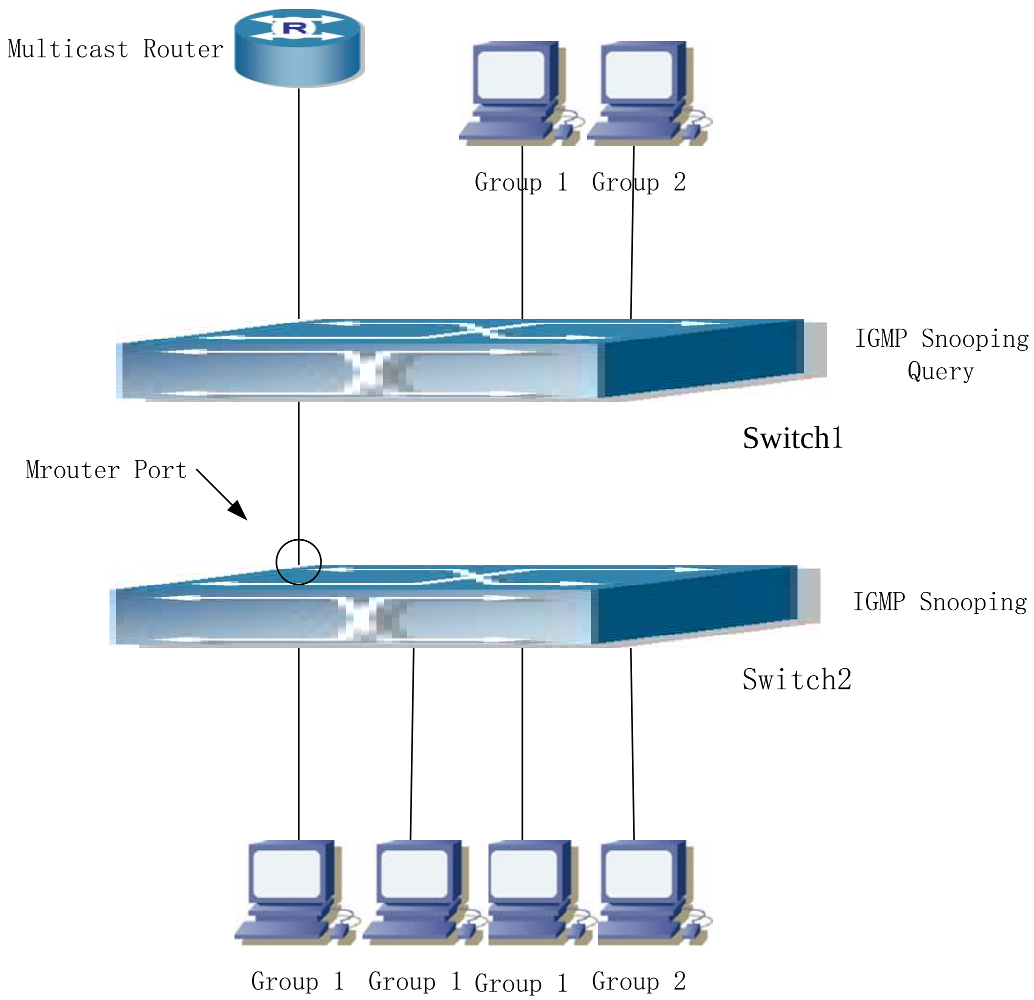


图 12-2　交换机作为 IGMP Querier 功能图

Switch2 的配置与案例 1 中 Switch 相同，交换机 Switch1 取代案例 1 中的 Multicast Router。假设其上配置 vlan 60 包含端口 1、2、15、19。端口 1 连接组播服务器，端口 2 连接 Switch2。为了定期发 Query，需要打开全局下的 igmp snooping 功能，同时在 vlan 60 上打开 igmp snooping query。

配置步骤如下：

SwitchA#config
SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 60 query

SwitchB#config
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 100
SwitchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 0/0/1

组播配置：
同案例 1。
IGMP snooping 侦听结果：
与案例 1 相似。

12.4 IGMP Snooping 排错帮助

12.4.1 监测和调试命令

12.4.1.1 show ip igmp snooping

命令：show ip igmp snooping [vlan <*vlan-id*>]
参数：<*vlan-id*>为指定要显示 IGMP Snooping 信息的 vlan 号。
命令模式：特权用户配置模式
使用指南：如果不指定 VLAN 号，则显示所有 VLAN 的 IGMP Snooping 和 Query 摘要信息。如果指定 VLAN 号，则显示该 VLAN 的 IGMP Snooping 和 Query 详细信息。
举例：
1.显示交换机的 IGMP Snooping 和 Query 摘要信息。

```
Switch#show ip igmp snooping
igmp snooping status                :Enabled
IGMP information for VLAN 1:

igmp snooping vlan status          :Disabled
igmp snooping vlan query            :Disabled
igmp snooping vlan mrouter port :(null)
--------------------------------

IGMP information for VLAN 2:

igmp snooping vlan status          :Enabled
igmp snooping vlan query            :Disabled
igmp snooping vlan mrouter port :(null)
--------------------------------

IGMP information for VLAN 3:

igmp snooping vlan status          :Disabled
igmp snooping vlan query            :Disabled
igmp snooping vlan mrouter port :(null)
--------------------------------
```

IGMP information for VLAN 4:
igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

IGMP information for VLAN 511:

igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

IGMP information for VLAN 5:

igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

显示内容	解释
igmp snooping status	交换机是否启动 igmp snooping 功能
igmp snooping vlan status	交换机的所有 vlan 的 igmp snooping 状态（是否启动）
igmp snooping vlan query	交换机的所有 vlan 的 query 状态（是否启动）
igmp snooping vlan mrouter port	交换机的所有 vlan 的 mrouter 端口号（如果有）
igmp snooping vlan mrouter state	交换机的所有 vlan 的 mrouter 端口状态（如果有），如果没有指定 mrouter 不会显示该表项

2.显示 VLAN2 的 IGMP Snooping 和 query 的详细信息。
Switch#show ip igmp snooping vlan 2
IGMP information for VLAN 2:

igmp snooping status :Enabled
igmp snooping vlan status :Enabled
igmp snooping vlan mrouter port : Ethernet0/0/4
igmp snooping vlan mrouter state :UP
igmp snooping vlan mrouter present: Yes
igmp snooping vlan immediate leave: No
igmp snooping vlan query :Disabled
igmp snooping vlan robustness :2
igmp snooping vlan query interval: 125
igmp snooping vlan query response time: 10
igmp snooping vlan query TX :0

```
igmp snooping vlan query SX        :2
igmp snooping multicast information:
MAC address                    Member port list
------------------------------------------------------------
01-00-5E-7F-28-B3          Ethernet0/0/5
------------------------------------------------------------
01-00-5E-7F-30-BD          Ethernet0/0/4    Ethernet0/0/5
```

```
Sort by port:

Port             State                 Type                   Group Address        Life
-------------------------------------------------------------------------
Ethernet0/0/4    MEMBERS_PRESENT    Snoop_Group_Addr    239.255.48.189        0
-------------------------------------------------------------------------
Ethernet0/0/5    MEMBERS_PRESENT    Snoop_Group_Addr    239.255.40.179        0
                 MEMBERS_PRESENT    Snoop_Group_Addr    239.255.48.189        0
-------------------------------------------------------------------------
```

显示内容	解释
igmp snooping status	交换机是否启动 igmp snooping 功能
igmp snooping vlan status	该 vlan 的 igmp snooping 状态（是否启动）
igmp snooping vlan query	该 vlan 的 query 状态（是否启动）
igmp snooping vlan mrouter port	该 vlan 的 mrouter 端口号（如果有）
igmp snooping vlan mrouter state	交换机的所有 vlan 的 mrouter 端口状态（如果有），如果没有指定 mrouter 不会显示该表项
igmp snooping vlan mrouter present	该 mrouter 是否收到 query 数据包
igmp snooping vlan query TX	该 vlan 发送 query 包的数量
igmp snooping vlan query SX	该 vlan 收到 query 包的数量
igmp snooping multicast mac	该 vlan igmp snooping 转发表学习到的组播地址
igmp snooping multicast port	该 vlan igmp snooping 转发表每个组播 mac 地址对应的成员端口名

12.4.1.2 show mac-address-table multicast

命令：show mac-address-table multicast [vlan <*vlan-id*>| igmp snooping]
功能：显示组播 MAC 地址表信息
参数：<*vlan-id*> 要显示的表项包含的 VLAN ID；**igmp snooping** 显示 IGMP snooping 学习到的组播地址
命令模式：特权用户配置模式
缺省情况：系统缺省不显示组播 MAC 地址与端口的映射。

使用指南：本命令显示当前交换机的组播
MAC 地址表信息

举例：显示 VLAN100 内的组播映射。

```
Switch(Config)#show mac-address-table multicast vlan 100
Vlan Mac Address                    Type       Ports
---- -------------------------- ------- -------------------------------------
100   01-00-5e-01-01-01              DYNAMIC Ethernet0/0/2
```

12.4.1.3 debug igmp snooping

命令：**debug ip igmp snooping**

no debug ip igmp snooping

功能：打开交换机的 IGMP Snooping 的调试开关；本命令的 no 操作为关闭该调试开关。

命令模式：特权用户配置模式

缺省情况：缺省关闭交换机的 IGMP Snooping 的调试开关。

使用指南：用来打开交换机 IGMP Snooping 调试开关，可以显示交换机处理 IGMP 数据包信息。

举例：打开 IGMP Snooping 调试打开。

Switch#debug ip igmp snooping

12.4.2 IGMP Snooping 排错帮助

- 交换机的 IGMP Snooping 功能和 IGMP Query 功能是互斥的，打开 Query 功能时就不能使用 Snooping 功能。因此用户在配置时需要明确配置的是 IGMP Snooping 功能还是 IGMP Query 功能。
- 当用户使用 IGMP Snooping 功能时，必须在相应的 VLAN 内指定 M-Router 端口；否则交换机不能进行正常的 IGMP Snooping。

第13章802.1x 配置

13.1 802.1x 介绍

IEEE 802.1x 是一种基于端口的网络接入控制技术，在局域网设备的物理接入级对接入设备进行认证和控制，此处的物理接入级指的是交换机设备的端口。连接在该类端口上的用户设备如果能通过认证，就可以访问局域网内的资源；如果不能通过认证，则无法访问局域网内的资源，相当于在物理上断开连接。

IEEE 802.1x 定义了基于端口的网络接入控制协议，需要注意的是该协议仅适用于接入设备与接入端口间点到点的连接方式，其中端口可以是物理端口，也可以是逻辑端口。典型的应用方式有：交换机的一个物理端口仅连接一个终端设备（基于物理端口）。

802.1x 的体系结构如下图：

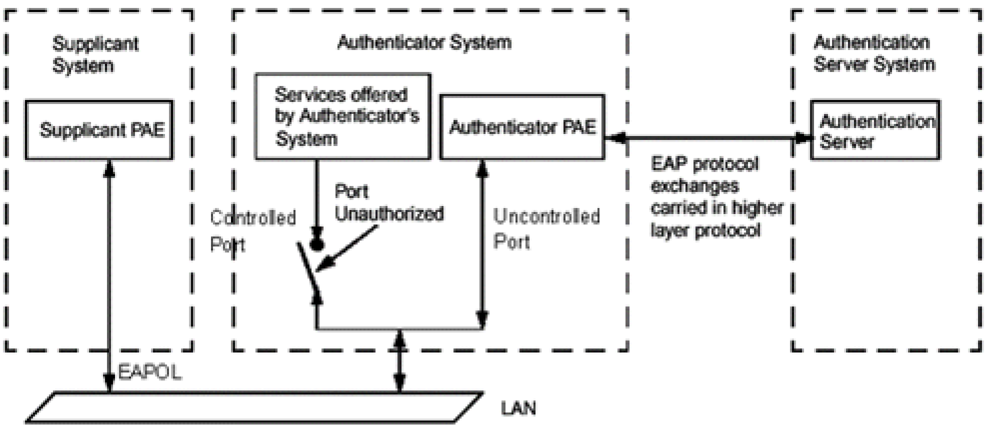


图 13-1 802.1x 体系结构

如上图所示 IEEE 802.1x 的体系结构中包括三个部分：

- Supplicant System，用户接入设备；
- Authenticator System，接入控制单元；
- Authentication Server System，认证服务器。

用户接入设备（PC）与接入控制单元（接入交换机）间运行 IEEE 802.1x 定义的 EAPOL 协议；接入控制单元与认证服务器间同样运行 EAP 协议，EAP 报文中封装了认证数据，该协议报文承载在其他高层次协议报文中，如 RADIUS，以便穿越复杂的网络到达认证服务器。

基于端口的网络接入控制将设备端为客户端提供服务的端口分为两个虚端口：受控端口和非受控端口。非受控端口始终处于双向连通状态，用于传递 EAP 认证报文。受控端口在授权状态下处于连通状态，用于传递业务报文；受控端口在非授权状态下处于关闭状态，禁止传递任何报文。

在神州数码交换机的 802.1x 的应用环境中，神州数码交换机作为接入控制单元；用户接入设备即是带有 802.1x 客户端软件的设备；认证服务器一般驻留在运营商的 AAA 中心，采用 Radius 服务器。

针对应用环境中存在一个物理端口下挂
接多个用户接入设备的情况，基于端口的 802.1x 认证不能区分各个用户接入设备，导致认证作用大打折扣。神州数码交换机实现了安全性和管理性更强的基于 MAC 地址的 802.1x 认证功能，对于同一物理端口下的用户接入设备，只有通过了认证的用户接入设备才能够接入网络，没有通过认证的用户接入设备不能接入网络。这样即使接入设备的一个物理端口下挂接多个终端，神州数码交换机仍然可以对每个用户接入设备进行单独认证和管理。

堆叠（stack）协议作为一种交换机管理技术，可将物理上的若干台交换机堆叠在一起，逻辑上当成一台交换机进行管理，神州数码交换机支持堆叠版本的 802.1x 功能，最大认证用户数可以达到 2000 人，推荐使用认证用户数不超过 1500 人。

13.2 堆叠端口介绍

目前，神州数码交换机支持 simplex 和 duplex 两种堆叠方式。堆叠交换机启动后，首先运行 MDP（Master Discovery Protocol）或 DDP（Duplex Discovery Protocol）选举一台交换机作为 MASTER，其它交换机作为 SLAVE。MASTER 负责管理所有 SLAVE 交换机，并负责为每台 SLAVE 分配一个 ID 号，MASTER 的 ID 为 0。SLAVE1 的 ID 为 1，依次类推。

堆叠后在 Radius Server 管理端所看到的端口号按如下方法计算：

交换机的 ID*64+所在的端口号

例如：对于认证端口为 Ethernet1/0/5 的用户，认证通过后，在管理端看到的该用户的端口号为：1*64+5=69；即该用户的端口号为 69。

注意：以上关于端口的计算不包括扩展槽位上的端口。

13.3 802.1x 配置

13.3.1 802.1x 配置任务序列

1. 使能交换机的 802.1x 功能；
2. 接入控制单元的属性配置
   1) 配置端口的授权状态
   2) 配置端口的接入控制方式：基于 MAC 地址还是基于端口
   3) 配置交换机 802.1x 的扩展功能
3. 与用户接入设备相关的属性配置（可选）
4. 与 RADIUS 服务器相关的属性配置
   1) 配置 RADIUS 认证密钥
   2) 配置 RADIUS 服务器
   3) 配置 RADIUS 服务的参数

1. 使能交换机的 802.1x 功能

命令	解释
全局配置模式	
aaa enable **no aaa enable**	使能交换机的 AAA 认证功能；本命令的 no 操作为关闭交换机的 AAA 认证功能。
aaa-accounting enable **no aaa-accounting enable**	使能交换机的计费功能；本命令的 no 操作为关闭交换机的计费功能。
dot1x enable **no dot1x enable**	使能交换机全局及端口的 802.1x 功能；本命令的 no 操作为关闭 802.1x 功能。
dot1x privateclient enable **no dot1x privateclient enable**	使能交换机强制客户端软件使用神州数码私有 802.1x 认证报文格式；本命令的 no 操作为关闭该功能，允许客户端软件使用标准 802.1x 认证报文格式。

2.接入控制单元的属性配置

1）配置端口的授权状态

命令	解释
端口配置模式	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	设置端口的 802.1x 授权状态，本命令的 no 操作用来恢复缺省配置。

2）配置端口的接入控制方式

命令	解释
端口配置模式	
dot1x port-method {macbased | portbased} **no dot1x port-method**	设置端口的接入控制方式；本命令的 no 操作用来恢复基于 MAC 地址的接入控制方式。
dot1x max-user <*number*> **no dot1x max-user**	设置指定端口最多允许接入的用户数；本命令的 no 操作为恢复缺省的最多允许 1 个用户。

3）配置交换机 802.1x 的扩展功能

命令	解释
全局配置模式	
dot1x macfilter enablebla **no dot1x macfilter enable**	打开交换机 802.1x 的地址过滤功能；本命令的 no 操作为关闭 802.1x 的地址过滤功能。
dot1x accept-mac <*mac-address*> [interface <*interface-name*>] **no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**	添加 802.1x 的地址过滤表的表项；本命令的 no 操作为删除 802.1x 的地址过滤表的表项。

dot1x eapor enable **no dot1x eapor enable**	打开交换机 EAP 中继的认证方式；本命令的 no 操作为采用 EAP 本地终结的认证方式。

3. 与 Supplicant 相关的属性配置

命令	解释
全局配置模式	
dot1x max-req <*count*> **no dot1x max-req**	设置交换机在没有收到 suppliant 回应而重新启动认证前，发送 EAP-request/MD5 帧的最大次数；本命令的 no 操作用来恢复缺省值。
dot1x re-authentication **no dot1x re-authentication**	设置允许对 suppliant 进行周期性重认证；本命令的 no 操作用来关闭该功能。
dot1x timeout quiet-period <*seconds*> **no dot1x timeout quiet-period**	设置在端口认证失败后保持静默状态的时间；本命令的 no 操作用来恢复缺省值。
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	设置交换机对 suppliant 重新认证的时间间隔；本命令的 no 操作用来恢复缺省值。
dot1x timeout tx-period <*seconds*> **no dot1x timeout tx-period**	设置交换机对 suppliant 重发 EAP-request/identity 帧的时间间隔；本命令的 no 操作用来恢复缺省值。
特权配置模式	
dot1x re-authenticate [interface <*interface-name*>]	设置对所有端口或某个指定端口进行 802.1x 重认证（不须等待超时）。

4.与 Authentication Server（RADIUS 服务器）相关的属性配置

1) 配置 RADIUS 认证密钥

命令	解释
全局配置模式	
radius-server key <*string*> **no radius-server key**	设置 RADIUS 服务器的密钥；本命令的 no 操作为删除 RADIUS 服务器的密钥。

2) 配置 RADIUS Server

命令	解释
全局配置模式	
radius-server authentication host <*IPaddress*> [[port {<*portNum*>}] [primary]] **no radius-server authentication host <*IPaddress*>**	配置 RADIUS 认证服务器的 IP 地址和监听端口号；本命令的 no 操作为删除 RADIUS 主机。

radius-server accounting host <IPaddress> [[port {<*portNum*>}] [primary]] **no radius-server accounting host <*IPaddress*>**	配置 RADIUS 计费服务器的 IP 地址和监听端口号；本命令的 no 操作为删除 RADIUS 主机。

3) 配置 RADIUS 服务参数

命令	解释
全局配置模式	
radius-server dead-time <*minutes*> **no radius-server dead-time**	配置 RADIUS 服务器 down 机后的恢复时间；本命令的 no 操作为恢复缺省配置。
radius-server retransmit <*retries*> **no radius-server retransmit**	配置 RADIUS 重传次数；本命令的 no 操作为恢复缺省配置。
radius-server timeout <*seconds*> **no radius-server timeout**	配置 RADIUS 服务器的超时定时器；本命令的 no 操作为恢复缺省配置。

13.3.2 802.1x 配置命令

13.3.2.1 aaa enable

命令：**aaa enable**

no aaa enable

功能：使能交换机 AAA 认证功能；本命令的 no 操作为关闭 AAA 认证功能。

命令模式：全局配置模式

参数：无

缺省情况：交换机不打开 AAA 认证功能。

使用指南：如果要实现交换机的 802.1x 认证功能，必须打开交换机的 AAA 认证功能。

举例：打开交换机的 AAA 功能。

Switch(Config)#aaa enable

13.3.2.2 aaa-accounting enable

命令：**aaa-accounting enable**

no aaa-accounting enable

功能：打开交换机的AAA计费功能；本命令的no 操作为关闭AAA 计费功能。

命令模式：全局配置模式

缺省情况：交换机不打开AAA计费功能。

使用指南：打开交换机的计费功能后，交换机将对认证者所在的端口的流量信息或上网时间进行计费。在计费开始时，交换机向 Radius 计费服务器发出计费开始的消息；并且每隔 5 秒钟针对在线用户向 Radius 计费服务器发一次计费包；在计费停止时，又向 Radius 计费服务器发送计费停止的消息。注意：只有当计费功能打开时，交换机在用户下线时才通知 Radius 计费服务器，用户的下线消息并不会通知 Radius 认证服务器。

举例：打开交换机的 AAA 计费功能。

Switch(Config)#aaa-accounting enable

13.3.2.3 dot1x accept-mac

命令：dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

功能：向 dot1x 地址过滤表中添加一个 MAC 地址表项，如果指定端口则添加的表项仅适用于指定端口，不指定端口则添加的表项适用于全部端口；本命令的 no 操作为删除 dot1x 的地址过滤表中的表项。

参数：<*mac-address*>为 MAC 地址；**<*interface-name*>**为接口名称及接口号；

命令模式：全局配置模式

缺省情况：无。

使用指南：交换机的 dot1x 地址过滤功能是根据 MAC 地址过滤表实现的，dot1x 地址过滤表由用户手工添加或删除。当添加 dot1x 地址过滤表项时指定了端口，则该地址过滤表项仅适用于该端口；若添加时未指定端口，则该地址过滤表项适用于交换机所有端口。当交换机的 dot1x 地址过滤功能打开，交换机会对认证者的 MAC 地址进行过滤，只有在 dot1x 地址过滤表中存在的客户发起的认证请求才能被接受，否则将被拒绝。

举例：将 MAC 地址 00-01-34-34-2e-0a 添加到 Ethernet 0/0/5 的过滤表中。

Switch(Config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 0/0/5

13.3.2.4 dot1x eapor enable

命令：dot1x eapor enable

no dot1x eapor enable

功能：设置交换机采用 EAP 中继的方式进行认证；本命令的 no 操作为设置交换机采用 EAP 本地终结的方式进行认证。

命令模式：全局配置模式

缺省情况：交换机采用 EAP 中继的方式进行认证。

使用指南：交换机与 Radius 认证服务器之间可能采用以太网方式连接或者采用 PPP 方式连接。如果交换机与 Radius 认证服务器之间采用以太网连接，那么交换机需要采用 EAP 中继的方式进行认证（即 EAPoR 认证）；如果交换机与 Radius 认证服务器之间采用 PPP 方式连接，则交换机需要采用 EAP 本地终结的方式进行认证（即 CHAP 认证）。根据交换机与认证服务器的连接方式的不同，交换机应该采用不同的认证方式进行认证。

举例：设置交换机采用 EAP 本地终结的方式进行认证。

Switch(Config)#no dot1x eapor enable

13.3.2.5 dot1x enable

命令：dot1x enable

no dot1x enable

功能：打开交换机全局及端口的 802.1x 功能；本命令的 no 操作为关闭 802.1x 功能。

命令模式：全局配置模式及端口配置模式

缺省情况：交换机在全局下不打开 802.1x 功能；若交换机在全局下打开 802.1x 功能，则端

口缺省也不打开 802.1x 功能。

使用指南：如果要对端口进行 802.1x 认证时，首先要打开全局下的 802.1x 功能，再在相应的端口下打开 802.1x 功能。如果该端口已经打开了 Spanning Tree，或者使能了 mac 绑定，或者是 Trunk 端口、端口聚合组的成员，则必须关闭端口下的 Spanning Tree 功能、或者关闭 mac 绑定、或者改变端口的为 Access 端口、取消参加端口汇聚组，否则无法打开端口下的 802.1x 功能。

举例：启动交换机的 802.1x 功能，并且打开 0/0/12 号端口 802.1x 功能。

Switch(Config)#dot1x enable
Switch(Config)#interface Ethernet 0/0/12
Switch(Config-Ethernet0/0/12)#dot1x enable

13.3.2.6 dot1x privateclient enable

命令：**dot1x privateclient enable**
no dot1x privateclient enable

功能：使能交换机强制客户端软件使用神州数码私有 802.1x 认证报文格式；本命令的 no 操作为关闭该功能，允许客户端软件使用标准 802.1x 认证报文格式。

命令模式：全局配置模式

缺省情况：交换机不支持私有 802.1x 认证报文。

使用指南：如果要实现神州数码整体解决方案，交换机必须使能支持神州数码私有 802.1x 认证报文，否则很多应用将不能使用，具体参见神州数码 DCBI 整体解决方案。交换机如果配置强制客户端软件使用神州数码私有 802.1x 认证报文格式，那么标准的 802.1x 客户端将不能通过认证。

举例：使能交换机强制客户端软件使用神州数码私有 802.1x 认证报文格式。

Switch(Config)#dot1x privateclient enable

13.3.2.7 dot1x macfilter enable

命令：**dot1x macfilter enable**
no dot1x macfilter enable

功能：打开交换机的 dot1x 地址过滤功能；本命令的 no 操作为关闭 dot1x 地址过滤功能。

命令模式：全局配置模式

缺省情况：交换机关闭 dot1x 地址过滤功能。

使用指南：当打开交换机的 dot1x 地址过滤功能，交换机会对认证者的 MAC 地址进行过滤，只有在 dot1x 地址过滤表中存在的客户发起的认证请求才能被接受。

举例：打开交换机的 MAC 地址过滤功能。

Switch(Config)#dot1x macfilter enable

13.3.2.8 dot1x max-req

命令：**dot1x max-req <*count*>**
no dot1x max-req

功能：设置交换机在没有收到 suppliant 回应而重新启动认证前，发送 EAP-request/MD5 帧的最大次数；本命令的 no 操作为恢复缺省值。

参数：***<count>*** 为发送 EAP-request/ MD5 帧的次数，取值范围为 1~10。
命令模式：全局配置模式
缺省情况：最大次数为 2 次。
使用指南：用户在配置发送 EAP-request/ MD5 帧的最大次数时，建议使用缺省值。
举例：更改 EAP-request/ MD5 帧的最大次数为 5 次。
Switch(Config)#dot1x max-req 5

13.3.2.9 dot1x max-user

命令：dot1x max-user <*number*>
no dot1x max-user
功能：设置指定端口最多允许接入的用户数；本命令的 no 操作为恢复缺省值。
参数：*<number>* 最多允许的接入用户数，取值范围为 1~254。
命令模式：端口配置模式。
缺省情况：每个端口缺省最多允许接入的用户数为 1。
使用指南：本命令只有在端口采用基于 MAC 地址的接入控制方式时才有效，若通过认证的 MAC 地址数量超过最多允许接入用户数，超出的用户将无法接入网络。
举例：设置端口 0/0/3 最多允许接入 5 个用户。
Switch(Config-Ethernet0/0/3)#dot1x max-user 5

13.3.2.10 dot1x port-control

命令：dot1x port-control {auto|force-authorized|force-unauthorized }
no dot1x port-control
功能：设置端口的 802.1x 授权状态；本命令的 no 操作为恢复缺省值。
参数：auto 为启动 802.1x 认证，根据交换机和 suppliant 之间的认证信息来确定端口处于已授权状态或者非授权状态；**force-authorized** 为设置端口为已授权状态，允许没有经过认证的数据通过该端口；**force-unauthorized** 为设置端口为非授权状态，交换机在该端口不提供对 suppliant 的认证服务，不允许任何数据通过该端口。
命令模式：端口配置模式
缺省情况：当打开端口的 802.1x 功能，端口缺省为 **force-authorized**。
使能指南：如果端口需要对用户进行 802.1x 认证，必须将端口认证状态设置为 **auto**。
举例：配置端口 1 为需要 802.1x 认证状态。
Switch(Config)#interface e 0/0/1
Switch(Config-Ethernet0/0/1)#dot1x port-control auto

13.3.2.11 dot1x port-method

命令：dot1x port-method {macbased | portbased}
no dot1x port-method
功能：设置指定端口的接入控制方式；本命令的 no 操作用来恢复缺省的接入控制方式。
参数：macbased 为基于 MAC 地址的接入控制方式；**portbased** 为基于端口的接入控制方式。

命令模式：端口配置模式

缺省情况：端口缺省使用基于 MAC 地址的接入控制方式。

使用指南：基于 MAC 地址的接入控制方式在安全性和管理性方面均比基于端口的接入控制方式要优越，建议只有在特殊情况下配置基于端口的接入控制方式。

举例：配置端口 0/0/4 采用基于端口的接入控制方式。

Switch(Config-Ethernet0/0/4)#dot1x port-method portbased

13.3.2.12 dot1x re-authenticate

命令：**dot1x re-authenticate [interface <*interface-name*>]**

功能：设置即时对所有端口或某个指定端口进行 802.1x 重认证，不必等待超时。

参数：**<*interface-name*>**为端口号，如果无参数则表示所有端口。

命令模式：特权配置模式

使用指南：本命令为特权模式下的命令，当配置本命令后，交换机立刻对客户端进行重认证，不需要等待重新认证定时器超时。认证之后，该命令就无效了。

举例：对端口 0/0/8 进行即时重认证。

Switch#dot1x re-authenticate interface ether 0/0/8

13.3.2.13 dot1x re-authentication

命令：**dot1x re-authentication**

no dot1x re-authentication

功能：设置允许对 suppliant 进行周期性重认证；本命令的 no 操作为关闭该功能。

命令模式：全局配置模式

缺省情况：缺省情况下周期性重认证功能是关闭的。

使用指南：当打开对 suppliant 的周期性重认证功能，交换机会周期性的对 suppliant 进行重新认证。一般情况下建议不打开周期性重认证功能。

举例：打开对认证者进行周期性重认证功能。

Switch(Config)#dot1x re-authentication

13.3.2.14 dot1x timeout quiet-period

命令：**dot1x timeout quiet-period <*seconds*>**

no dot1x timeout quiet-period

功能：设置 suppliant 在认证失败后端口保持静默状态的时间；本命令的 no 操作为恢复缺省值。

参数：**<*seconds*>**为端口保持静默状态的时间长度值，单位为秒，取值范围为 1~65535。

命令模式：全局配置模式

缺省情况：缺省为 10 秒。

使用指南：建议使用缺省值。

举例：设置静默时间为 120 秒。

Switch(Config)#dot1x timeout quiet-period 120

13.3.2.15 dot1x timeout re-authperiod

命令：dot1x timeout re-authperiod <*seconds*>
no dot1x timeout re-authperiod
功能：设置交换机对 suppliant 重认证的时间间隔；本命令的 no 操作为恢复缺省值。
参数：<*seconds*>重认证的时间间隔，单位为秒，取值范围为 1~65535。
命令模式：全局配置模式
缺省情况：缺省为 3600 秒。
使用指南：在修改交换机对 suppliant 的重认证时间间隔时，必须首先打开 dot1x re-authentication。如果没有配置交换机的重认证功能,那么所设置交换机对 suppliant 重认证的时间间隔将不起作用
举例：设置重认证时间为 1200 秒。
Switch(Config)#dot1x timeout re-authperiod 1200

13.3.2.16 dot1x timeout tx-period

命令：dot1x timeout tx-period <*seconds*>
no dot1x timeout tx-period
功能：设置交换机对 suppliant 重发 EAP-request/identity 帧的时间间隔；本命令的 no 操作为恢复缺省值。
参数：<*seconds*>为重新发送 EAP 请求帧的时间间隔，单位为秒，取值范围为 1~65535。
命令模式：全局配置模式
缺省情况：缺省为 30 秒。
使用指南：建议使用缺省值。
举例：更改重新发送 EAP 请求帧的时间间隔为 1200 秒。
Switch(Config)#dot1x timeout tx-period 1200

13.3.2.17 radius-server accounting host

命令：radius-server accounting host <*ip-address*> [port <*port-number*>] [primary]
no radius-server accounting host <*ip-address*>
功能：设置RADIUS计费服务器IP地址和监听端口号；本命令的no操作为删除RADIUS 计费服务器。
参数：<*ip-address*>服务器的IP 地址；**<*port-number*>** 为服务器的监听端口号，取值范围为：0~65535；**primary**为主用服务器，在配置RADIUS服务器时，可以配置多个，使用顺序在没有配置**primary**时，按配置顺序查找可以使用的RADIUS服务器；如果配置**primary**，则首先使用这个RADIUS服务器。
命令模式：全局配置模式
缺省情况：系统没有设置RADIUS计费服务器。
使用指南：本命令用于指定与交换机进行计费的 RADIUS 服务器的 IP 地址和端口号，可以配置多条该命令。其中参数**<*port-number*>**用于指定计费端口号，该端口号必须与指定的 RADIUS 服务器上的计费端口号相同，缺省为 1813，若将该端口号配置为 0，计费端口

随机产生，可能导致配置无效。本命令可以反
复配置多条以指定多台与交换机建立通讯关系的 RADIUS 服务器，交换机将向所有配置好的计费服务器发送计费报文，所配置的这些计费服务器可以相互做为备份服务器。如果配置 **primary**，则将此 RADIUS 服务器作为主用服务器。
举例：设置 RADIUS 计费服务器的 IP 地址为 100.100.100.60，端口号为 3000，并作为主用服务器。
Switch(Config)#radius-server accounting host 100.100.100.60 port 3000 primary

13.3.2.18 radius-server authentication host

命令：**radius-server authentication host <*ip-address*> [port <*port-number*>] [primary]**
no radius-server authentication host <*ip-address*>
功能：设置 RADIUS 服务器 IP 地址和监听端口号；本命令的 no 操作为删除 RADIUS 认证服务器。
参数：**<*ip-address*>**服务器的 IP 地址；**<*port-number*>**为服务器的监听端口号，取值范围为 0~65535，其中 0 表示不作认证服务器使用；**primary** 为主用服务器。
命令模式：全局配置模式
缺省情况：系统没有设置 RADIUS 认证服务器。
使用指南：本命令用于指定与交换机进行认证的 RADIUS 服务器的 IP 地址和端口号，可以配置多条该命令。其中参数 port 用于指定认证端口号，该端口号必须与指定的 RADIUS 服务器上的认证端口号相同，缺省为 1812，若将该端口号配置为 0 则认为该指定的服务器没有认证功能。本命令可以反复配置多条以指定多台与交换机建立通讯关系的 RADIUS 服务器，其中以配置的顺序作为交换机认证服务器的顺序。如果配置 **primary**，则将此 RADIUS 服务器作为主用服务器。
举例：配置 RADIUS 认证服务器地址为 200.1.1.1。
Switch(Config)#radius-server authentication host 200.1.1.1

13.3.2.19 radius-server dead-time

命令：**radius-server dead-time <*minutes*>**
no radius-server dead-time
功能：设置 RADIUS 服务器死机后的恢复时间；本命令的 no 操作为恢复缺省配置。
参数：**<*minutes*>**为 RADIUS 服务器死机的恢复时间值，单位为分钟，取值范围为 1~255。
命令模式：全局配置模式
缺省情况：缺省为 5 分钟。
使用指南：本命令指定交换机等待 RADIUS 服务器由不可访问状态恢复为可以访问状态的时间。交换机查知该服务器不能访问时，交换机将该服务器状态设置成无效状态，超过上述配置间隔时间后，系统将认证服务器状态设置成有效。
举例：配置 RADIUS 服务器死机后的恢复时间为 3 分钟。
Switch(Config)#radius-server dead-time 3

13.3.2.20 radius-server key

命令：radius-server key <*string*>

no radius-server key

功能：设置 RADIUS 服务器（包括认证和计费）的密钥；本命令的 no 操作为删除 RADIUS 服务器的密钥。

参数：<*string*>为 RADIUS 服务器的密钥字符串，取值范围不超过 16 个字符。

命令模式：全局配置模式

使用指南：该密钥为交换机与设置的 RADIUS 服务器进行加密的报文通信使用。该设置的密钥必须与交换机设置的 RADIUS 服务器上的密钥相同，否则将不能进行正确的 RADIUS 认证和计费。

举例：配置 RADIUS 认证密钥为 test。

Switch(Config)# radius-server key test

13.3.2.21 radius-server retransmit

命令：radius-server retransmit <*retries*>

no radius-server retransmit

功能：设置 RADIUS 认证报文的重传次数；本命令的 no 操作为恢复缺省配置。

参数：<*retries*>为 RADIUS 服务器的重传次数，取值范围为 0~100。

命令模式：全局配置模式

缺省情况：缺省为 3 次。

使用指南：本命令指定交换机向 RADIUS 服务器发送数据包后，接收不到 RADIUS 服务器的回应需要重新发送该数据包的次数。在没有收到认证服务器发送的认证信息时，需向认证服务器重传 AAA 的认证请求。重传 AAA 请求计数达到设定的重传次数并仍没有接收到服务器的回应后，认为该服务器已不能正常工作，交换机将该服务器设置为不可访问状态。

举例：配置 RADIUS 认证报文重传次数为 5 次。

Switch(Config)# radius-server retransmit 5

13.3.2.22 radius-server timeout

命令：radius-server timeout <*seconds*>

no radius-server timeout

功能：设置 RADIUS 服务器超时定时器；本命令的 no 操作为恢复缺省配置。

参数：<*seconds*>为 RADIUS 服务器超时定时器值，单位为秒，取值范围为 1~1000。

命令模式：全局配置模式

缺省情况：缺省为 3 秒。

使用指南：本命令指定交换机等待 RADIUS 服务器响应的时间间隔。交换机发送给 RADIUS Server 的请求数据包后，等待接收相应的响应数据包。若在规定的等待时间内没有接收到 RADIUS 服务器的回应，则根据当时的状态重新发送请求数据包或将该服务器状态设置为不可访问。

举例：配置 radius 服务器超时定时器为 30 秒。

Switch(Config)# radius-server timeout 30

13.4 802.1x 应用举例

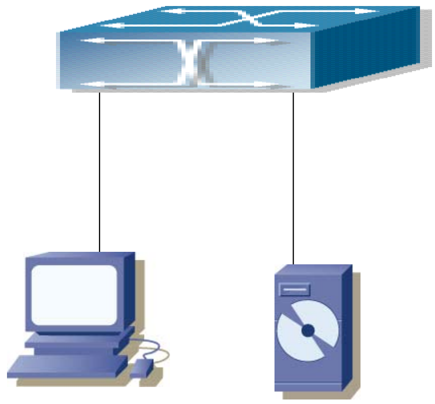


图 13-2 IEEE802.1x 配置举例拓扑图

计算机连接到交换机的端口 0/0/2 上，端口 0/0/2 开启 IEEE802.1x 认证功能，接入方式采用缺省的基于 MAC 地址认证方式。交换机的 IP 地址设置为 10.1.1.2，并将除端口 0/0/2 以外的任意一个端口与 RADIUS 认证服务器相连接，RADIUS 认证服务器的 IP 地址设置为 10.1.1.3，认证、计费端口为缺省端口 1812 和端口 1813。计算机上安装神州数码 IEEE802.1x 认证客户端软件，并通过使用此软件来实现 IEEE802.1x 认证。

配置步骤如下：

```
Switch(Config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(Config)#radius-server authentication host 10.1.1.3
Switch(Config)#radius-server accounting host 10.1.1.3
Switch(Config)#radius-server key test
Switch(Config)#aaa enable
Switch(Config)#aaa-accounting enable
Switch(Config)#dot1x enable
Switch(Config)#interface ethernet 0/0/2
Switch(Config-Ethernet0/0/1)#dot1x enable
Switch(Config-Ethernet0/0/1)#dot1x port-control auto
Switch(Config-Ethernet0/0/1)#exit
```

13.5 802.1x 排错帮助

13.5.1 802.1x 调试和监测命令

13.5.1.1 show aaa config

命令：show aaa config
功能：显示交换机作为RADIUS客户端已经有的配置命令。
命令模式：特权模式
使用指南：显示交换机是否打开aaa认证、计费功能，及密钥，认证、计费服务器的信息等。
举例：
Switch#show aaa config（如果是布尔量，1 代表 TRUE，0 代表 FALSE）

```
----------------- AAA config data ------------------

    Is Aaa Enabled = 1
    Is Account Enabled= 1
    MD5 Server Key = aa
    authentication server sum = 2
    authentication server[0].Host IP = 30.1.1.30
                                     .Udp Port = 1812
                                     .Is Primary = 1
                                     .Is Server Dead = 0
                                     .Socket No = 0
    authentication server[1].Host IP = 192.168.1.218
                                     .Udp Port = 1812
                                     .Is Primary = 0
                                     .Is Server Dead = 0
                                     .Socket No = 0
    accounting server sum = 2
    accounting server[0].Host IP = 30.1.1.30
                                 .Udp Port = 1813
                                 .Is Primary = 1
                                 .Is Server Dead = 0
                                 .Socket No = 0
    accounting server[1].Host IP = 192.168.1.218
                                 .Udp Port = 1813
                                 .Is Primary = 0
                                 .Is Server Dead = 0
                                 .Socket No = 0
    Time Out = 3
    Retransmit = 3
```

Dead Time = 5
Account Time Interval = 0

显示内容	描述
Is Aaa Enabled	显示 AAA 认证功能是否打开。1 为打开；0 为关闭；
Is Account Enabled	显示 AAA 计费功能是否打开。1 为打开；0 为关闭；
MD5 Server Key	显示 RADIUS 服务器的密钥；
authentication server sum	认证服务器的个数；
authentication server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	显示认证服务器号及对应的 IP 地址、UDP 端口号、是否是 Primary 服务器、是否宕机、Socket 号；
accounting server sum	计费服务器的个数；
accounting server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	显示计费服务器号及对应的 IP 地址、UDP 端口号、是否是 Primary 服务器、是否 down 机、Socket 号；
Time Out	显示 RADIUS 服务器的超时定时器；
Retransmit	显示 RADIUS 服务器认证报文的重传次数；
Dead Time	显示 RADIUS 服务器宕机后的恢复时间；
Account Time Interval	显示计费时间间隔。

13.5.1.2 show aaa authenticated-user

命令：show aaa authenticated-user
功能：显示已经通过认证的在线用户。
命令模式：特权模式
使用指南：一般只关心在线用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。
举例：

```
Switch#show aaa authenticated-user
------------------------- authenticated users -------------------------------
    User-name        Retry-time      Radius-ID        Port     Eap-ID   Chap-ID   Mem-Addr
WaitingNum
----------------------------------------------------------------------------
  bb                      0             4             2       0        1      16652824        0
```

13.5.1.3 show aaa authenticating-user

命令：show aaa authenticating-user

功能：显示正在进行认证的用户。
命令模式：特权模式
使用指南：一般只关心正在进行认证用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。
举例：

```
Switch#show aaa authenticating-user
------------------------ authenticating users ------------------------------
    User-name      Retry-time      Radius-ID       Port      Eap-ID   Chap-ID   Mem-Addr
WaitingNum
---------------------------------------------------------------------------
   bb                  0            4             2       1          0      16652824       0
```

13.5.1.4 show radius count

命令：**show radius {authencated-user|authencating-user} count**
功能：显示 radius 认证用户的统计信息。
参数：authencated-user：显示已经通过认证的在线用户；authencating-user：正在进行认证的用户。
命令模式：特权配置模式
使用指南：通过 show radius count 命令可以查看 radius 认证用户的相关统计信息.
举例：
1.显示有关 radius 认证通过用户的统计信息.

```
Switch #show radius authencated-user count
        -------------------- Radius user statistic---------------------
The authencated online user num is:         1
 The total user num is:           1
```

2.显示 radius 正在认证用户及其它情况用户的统计信息

```
Switch #sho radius authencating-user count
        -------------------- Radius user statistic---------------------
The authencating user num is:            0
The stopping user num is:          0
The stopped user num is:          0
The total user num is:          1
```

13.5.1.5 show dot1x

命令：**show dot1x [interface <*interface-list*>]**
功能：显示有关 dot1x 参数信息，如果后面增加参数信息，则显示相应端口的 dot1x 的状态。
参数：***<interface-list>***为端口列表。如果无参数，则显示所有端口信息
命令模式：特权配置模式
使用指南：通过 show dot1x 命令可以查看端口的 dot1x 的相关参数以及端口的 dot1x 的信息。
举例：
1.显示交换机的 dot1x 全局参数信息。

```
Switch#show dot1x
Global 802.1x Parameters
   reauth-enabled            no
   reauth-period             3600
   quiet-period              10
   tx-period                 30
   max-req                   2
   authenticator mode        passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable

802.1x is enabled on ethernet 1
Authentication Method:Port based
   Status                    Authorized
   Port-control              Auto
   Supplicant                00-03-0F-FE-2E-D3

Authenticator State Machine
   State                     Authenticated

Backend State Machine
   State                     Idle

Reauthentication State Machine
   State                     Stop
```

显示内容	解释
Global 802.1x Parameters	全局 802.1x 参数信息
reauth-enabled	交换机是否打开重认证功能
reauth-period	重认证时间间隔
quiet-period	静默时间间隔
tx-period	EAP 数据包重传时间间隔
max-req	EAP 数据包重传次数
authenticator mode	交换机认证模式
Mac Filter	交换机是否使能 dot1x 地址过滤功能
MacAccessList :	Dot1x 地址过滤表
dot1x-EAPoR	交换机采用的认证方式（EAP 中继 、EAP 本地终结）
802.1x is enabled on ethernet 1	显示端口的 dot1x 是否打开
Authentication Method:	端口认证方式（基于 MAC，基于端口）
Status	端口认证状态
Port-control	端口授权状态
Supplicant	认证者 MAC 地址

Authenticator State Machine	Authenticator 状态机状态
Backend State Machine	Backend 状态机状态
Reauthentication State Machine	Reauthentication 状态机状态

13.5.1.6 debug aaa

命令：**debug aaa**

no debug aaa

功能：打开 aaa 的调试信息；本命令的 no 操作为关闭 aaa 的调试信息。
命令模式：特权配置模式
参数：无
使用指南：打开 aaa 调试信息，可以查看 Radius 协议的协商过程，在遇到故障时有助于监测故障原因。
举例：打开 aaa 调试信息。
Switch#debug aaa

13.5.1.7 debug dot1x

命令：**debug dot1x**

no debug dot1x

功能：打开 dot1x 的调试信息；本命令的 no 操作为关闭 dot1x 的调试信息。
命令模式：特权配置模式
参数：无
使用指南：打开 dot1x 调试信息，可以查看 dot1x 协议的协商过程，在遇到故障时有助于监测故障原因。
举例：打开 dot1x 调试信息。
Switch#debug dot1x

13.5.2 802.1x 排错帮助

用户在使用 802.1x 时，通常会遇到端口无法配置 802.1x；或者 802.1x 认证状态为 auto，用户运行 802.1x 的 suppliant 软件后，端口仍不能改变为认证通过状态的情况。可能的原因及解决建议如下：

- 如果出现端口无法配置 802.1x 的情况，请检查交换机的认证端口是否运行了 Spanning-tree，或者端口 mac 绑定，或者端口已经配置为 Trunk 端口、聚合端口。如果要打开端口的 802.1x 认证功能，则必须关闭该端口下的上述功能。
- 如果交换机配置正确，但认证仍无法通过，请检查交换机与 RADIUS 服务器，交换机与 802.1x 客户机之间是否相互连通；检查交换机端口 VLAN 的配置。
- 通过查看 RADIUS 服务器的事件日志，判断问题的起因。在事件日志中对登录不成功的不仅有记录还有不成功原因的提示。如事件日志显示 authenticator 的登录口令不对，则修改 radius-server key 参数；如果事件日志中显示没有该 authenticator，则需在

RADIUS 服务器中增加该 authenticator；
如事件日志中提示没有该登录用户，说明用户的登录名和口令有误，输入正确的用户名和口令。

第14章ACL 配置

14.1 ACL 介绍

ACL (Access Control Lists)是交换机实现的一种数据包过滤机制，通过允许或拒绝特定的数据包进出网络，交换机可以对网络访问进行控制，有效保证网络的安全运行。用户可以基于报文中的特定信息制定一组规则（rule），每条规则都描述了对匹配一定信息的数据包所采取的动作：允许通过（permit）或拒绝通过（deny）。用户可以把这些规则应用到特定交换机端口的入口或出口方向，这样特定端口上特定方向的数据流就必须依照指定的ACL规则进出交换机。

14.2 Access-list

Access-list是一个有序的语句集，每一条语句对应一条特定的规则(rule)。每条rule包括了过滤信息及匹配此rule时应采取的动作。Rule包含的信息可以包括源MAC、目的MAC、源IP、目的IP、IP协议号、tcp端口等条件的有效组合。根据不同的标准，access-list可以有如下分类：

- 根据过滤信息：ip access-list（三层以上信息），mac access-list（二层信息），mac-ip access-list（二层以上信息）。
- 根据配置的复杂程度：标准(standard)和扩展(extended)，扩展方式可以指定更加细致过滤信息。
- 根据命名方式：数字(numbered)和命名(named)。

对一条ACL的说明应当从这三个方面加以描述。

14.2.1 Access-group

当用户按照实际需要制定了一组access-list之后，就可以把他们分别应用到不同端口的不同方向上。access-group就是对特定的一条access-list与特定端口的特定方向的绑定关系的描述。当您建立了一条access-group之后，流经此端口此方向的所有数据包都会试图匹配指定的access-list规则，以决定交换动作是允许(permit)或拒绝(deny)。另外还可以在端口加上对ACL规则统计计数器，以便统计流经端口的符合ACL规则数据包的数量。

14.2.2 Access-list 动作及全局默认动作

Access-list动作及默认动作分为两种：允许通过(permit)或拒绝通过(deny)。具体有如下：

- 在一个access-list内，可以有多条规则（rule）。对数据包的过滤从第一条规则（rule）开始，直到匹配到一条规则（rule），其后的规则（rule）不再进行匹配。

- 全局默认动作只对端口入口方向的IP包
  有效。对入口的非IP数据包以及出口的所有数据包，其默认转发动作均为允许通过(permit)。
- 只有在包过滤功能打开且端口上没有绑定任何的ACL或不匹配任何绑定的ACL时才会匹配入口的全局的默认动作。
- 当一条access-list被绑定到一个端口的出方向时，其规则（rule）的动作只能为拒绝通过（deny）。

14.3 ACL 配置

14.3.1 ACL 配置任务序列

1. 配置 access-list

（1） 配置数字标准 IP 访问列表

（2） 配置数字扩展 IP 访问列表

（3） 配置命名标准 IP 访问列表

  a) 创建一个命名标准 IP 访问列表
  b) 指定多条 permit 或 deny 规则表项
  c) 退出访问表配置模式

（4） 配置命名扩展 IP 访问列表

  a) 创建一个命名扩展 IP 访问列表
  b) 指定多条 permit 或 deny 规则表项
  c) 退出访问表配置模式

（5） 配置数字标准 MAC 访问列表

（6） 配置数字扩展 MAC 访问列表

（7） 配置命名扩展 MAC 访问列表

  a) 创建一个命名扩展 MAC 访问列表
  b) 指定多条 permit 或 deny 规则表项
  c) 退出 MAC 访问表配置模式

（8） 配置数字扩展 MAC-IP 访问列表

（9） 配置命名扩展 MAC-IP 访问列表

  a) 创建一个命名扩展 MAC-IP 访问列表
  b) 指定多条 permit 或 deny 规则表项
  c) 退出 MAC-IP 访问表配置模式

2. 配置包过滤功能

（1）全局打开包过滤功能

（2）配置默认动作(default action)

3. 配置时间范围功能

（1） 创建时间范围名称

（2） 配置周期性时段

（3） 配置绝对性时段

4. 将 accessl-list 绑定到特定端口的特定方向
5. 清空指定接口的包过滤统计信息

1. 配置 access-list

（1）配置数字标准 IP 访问列表

命令	解释
全局配置模式	
access-list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} **no access-list <*num*>**	创建一条数字标准 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的 no 操作为删除一条数字标准 IP 访问列表。

（2）配置数字扩展 IP 访问列表

命令	解释
全局配置模式	
access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 icmp 数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 igmp 数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [sPort <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [dPort <*dPort*>] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 tcp 数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [sPort <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [dPort <*dPort*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 udp 数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条匹配其他特定 IP 协议或所有 IP 协议的数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
no access-list <*num*>	删除一条数字扩展 IP 访问列表。

（**3**）配置命名标准 **IP** 访问列表

a. 创建一个命名标准 **IP** 访问列表

命令	解释
全局配置模式	
ip access-list standard <*name*> **no ip access-list standard <*name*>**	创建一条命名标准 IP 访问列表；本命令的 no 操作为删除此命名标准 IP 访问列表。

b. 指定多条 **permit** 或 **deny** 规则

命令	解释
命名标准 IP 访问列表配置模式	
[no] {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}	创建一条命名标准 IP 访问规则（rule）；本命令的 no 操作为删除此命名标准 IP 访问规则（rule）。

c. 退出命名标准 **IP** 访问列表配置模式

命令	解释
命名标准 IP 访问列表配置模式	
Exit	退出命名标准 IP 访问列表配置模式。

（**4**）配置命名扩展 **IP** 访问列表

a. 创建一个命名扩展 **IP** 访问列表

命令	解释
全局配置模式	
ip access-list extended <*name*> **no ip access-list extended <*name*>**	创建一条命名扩展 IP 访问列表；本命令的 no 操作为删除此命名扩展 IP 访问列表。

b. 指定多条 **permit** 或 **deny** 规则

命令	解释
命名扩展 IP 访问列表配置模式	
[no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 icmp 命名扩展 IP 访问规则（rule）；本命令的 no 操作为删除此命名扩展 IP 访问规则（rule）。

[no] {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	创建一条 igmp 命名扩展 IP 访问规则（rule）；本命令的 no 操作为删除此命名扩展 IP 访问规则（rule）。
[no] {deny | permit} tcp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [sPort <sPort>] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [dPort <dPort>] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	创建一条 tcp 命名扩展 IP 访问规则（rule）；本命令的 no 操作为删除此命名扩展 IP 访问规则（rule）。
[no] {deny | permit} udp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [sPort <sPort>] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [dPort <dPort>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	创建一条 udp 命名扩展 IP 访问规则（rule）；本命令的 no 操作为删除此命名扩展 IP 访问规则（rule）。
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <int>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]	创建一条匹配其他特定 IP 协议或所有 IP 协议的数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。

c. 退出命名扩展 IP 访问列表配置模式

命令	解释
命名扩展 IP 访问列表配置模式	
Exit	退出命名扩展 IP 访问列表配置模式。

（5） 配置数字标准 MAC 访问列表

命令	解释
全局配置模式	
access-list <num> {deny|permit} {any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} **no access-list <num>**	创建一条数字标准 mac 访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的 no 操作为删除一条数字标准 mac 访问列表。

（6） 配置数字扩展 MAC 访问列表

<table>
<tr><td>命令</td><td>解释</td></tr>
<tr><td>全局配置模式</td><td></td></tr>
<tr><td>access-list <num> {deny|permit} {any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}[{untagged-eth2|tagged-eth2|untagged-802.3|tagged-802.3} [<offset1> <length1> <value1> [<offset2> <length2> <value2> [<offset3> <length3> <value3> [<offset4> <length4> <value4>]]]]]
no access-list <num></td><td>创建一条数字扩展 mac 访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的no操作为删除一条数字扩展 mac 访问列表。</td></tr>
</table>

（7） 配置命名扩展 MAC 访问列表

a. 创建一个命名扩展 MAC 访问列表

<table>
<tr><td>命令</td><td>解释</td></tr>
<tr><td>全局配置模式</td><td></td></tr>
<tr><td>Mac-access-list extended <name>
no mac-access-list extended <name></td><td>创建一条命名扩展 MAC 访问列表；本命令的 no 操作为删除此命名扩展 MAC 访问列表。</td></tr>
</table>

b. 指定多条 permit 或 deny 规则表项

<table>
<tr><td>命令</td><td>解释</td></tr>
<tr><td>命名扩展 MAC 访问列表配置模式</td><td></td></tr>
<tr><td>[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac> <dmac-mask>}} [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]</td><td>创建一条匹配普通 MAC 帧的命名扩展 MAC 访问规则(rule)；no 操作为删除此命名扩展 MAC 访问规则（rule）</td></tr>
<tr><td>[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}} [untagged-eth2 [ethertype <protocol> [protocol-mask]]]</td><td>创建一条匹配 untagged 以太网 2 帧类型的命名扩展 MAC 访问规则(rule)； no 操作为删除此命名扩展 MAC 访问规则（rule）</td></tr>
<tr><td>[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} [untagged-802.3]</td><td>创建一条匹配 untagged 802.3 帧类型的 MAC 访问规则(rule)； no 操作为删除此命名扩展 MAC 访问规则（rule）</td></tr>
</table>

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype<*protocol*> [<*protocol-mask*>]]]	创建一条匹配 tagged 以太网 2 帧类型的 MAC 访问规则(rule)；no 操作为删除此命名扩展 MAC 访问规则（rule）
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [tagged-802.3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]	创建一条匹配 tagged 802.3 帧类型的 MAC 访问规则(rule)；no 操作为删除此命名扩展 MAC 访问规则（rule）

c. **退出 MAC 访问表配置模式**

命令	解释
命名扩展 MAC 访问列表配置模式	
Exit	退出命名扩展 MAC 访问列表配置模式

（8）配置数字扩展 MAC-IP 访问列表

命令	解释
全局配置模式	
access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 mac-icmp 数字扩展mac-ip访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 mac-igmp 数字扩展mac-ip访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。

access-list<num>{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}[s-port<port1>] {{<destination><destination-wildcard>}|any-destination|{host-destination <destination-host-ip>}} [d-port <port3>] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<*time-range-name*>]	创建一条 mac-tcp 数字扩展mac-ip访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}[s-port<*port1*>] {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination<*destination-host-ip*>}} [d-port <*port3*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条mac-udp数字扩展mac-ip访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条匹配其他特定 mac-IP 协议或所有 mac-IP 协议的数字扩展mac-ip访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。
no access-list <*num*>	删除一条数字扩展MAC-IP 访问列表。

（**9**）配置命名扩展 **MAC-IP** 访问列表

a) 创建一个命名扩展 **MAC-IP** 访问列表

命令	解释
全局配置模式	
Mac-ip-access-list extended <*name*> **no Mac-ip-access-list extended <*name*>**	创建一条命名扩展 MAC-IP 访问列表；本命令的 no 操作为删除此命名扩展 MAC-IP 访问列表。

b) 指定多条 **permit** 或 **deny** 规则表项

<table>
<tr><th>命令</th><th>解释</th></tr>
<tr><td>命名扩展 MAC-IP 访问列表配置模式</td><td></td></tr>
<tr><td>[no] {deny|permit} {any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}icmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]</td><td>创建一条 mac-icmp 命名扩展 MAC-IP 访问规则（rule）；no 操作为删除此命名扩展 IP 访问规则（rule）。</td></tr>
<tr><td>[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]</td><td>创建一条 mac-igmp 命名扩展 MAC-IP 访问规则（rule）； no 操作为删除此命名扩展 IP 访问规则（rule）。</td></tr>
<tr><td>[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}}[s-port<port1>] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port <port3>] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]</td><td>创建一条 mac-tcp 命名扩展 MAC-IP 访问规则（rule）；no 操作为删除此命名扩展 IP 访问规则（rule）。</td></tr>
<tr><td>[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}udp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}}[s-port<port1>] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port <port3>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]</td><td>创建一条 mac-udp 命名扩展 MAC-IP 访问规则（rule）；no 操作为删除此命名扩展 IP 访问规则（rule）。</td></tr>
</table>

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	创建一条 mac-ip 其他协议类型的命名扩展 MAC-IP 访问规则（rule）；no 操作为删除此命名扩展 IP 访问规则（rule）。

c) 退出 **MAC-IP** 访问表配置模式

命令	解释
命名扩展 MAC-IP 访问列表配置模式	
Exit	退出命名扩展 MAC-IP 访问列表配置模式

2. 配置包过滤功能

（**1**）全局打开包过滤功能

命令	解释
全局配置模式	
firewall enable	全局打开包过滤功能。
firewall disable	全局关闭包过滤功能。

（**2**）配置默认动作**(default action)**

命令	解释
全局配置模式	
firewall default permit	设置默认动作为 permit。
firewall default deny	设置默认动作为 deny。

3. 配置时间范围功能

（**1**）创建时间范围名称

命令	解释
全局配置模式	
time-range <*time_range_name*>	创建一个名为 ***time_range_name*** 的时间范围名
no time-range <*time_range_name*>	停止名为 ***time_range_name*** 的时间范围功能

（**2**）配置周期性时段

命令	解释
时间范围模式	

<table>
<tr><td>absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<<i>start_time</i>>to {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <<i>end_time</i>></td><td rowspan="2">配置一周内的各种不同要求的时间范围，每周都循环这个时间</td></tr>
<tr><td>periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}| daily| weekdays | weekend} <<i>start_time</i>> to <<i>end_time</i>></td></tr>
<tr><td>[no]absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<<i>start_time</i>> to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday| Sunday} <<i>end_time</i>></td><td rowspan="2">停止一周内的时间范围配置</td></tr>
<tr><td>[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily|weekdays| weekend} <<i>start_time</i>> to <<i>end_time</i>></td></tr>
</table>

（3）配置绝对性时段

<table>
<tr><td>命令</td><td>解释</td></tr>
<tr><td>全局配置模式</td><td></td></tr>
<tr><td>Absolute start<<i>start_time</i>><<i>start_data</i>>[end<<i>end_time</i>> <<i>end_data</i>>]</td><td>创建一个绝对时间范围</td></tr>
<tr><td>[no]absolute start<<i>start_time</i>><<i>start_data</i>>[end<<i>end_time</i>><<i>end_data</i>>]</td><td>停止一个绝对时间范围功能</td></tr>
</table>

4. 将 accessl-list 绑定到特定端口的特定方向

<table>
<tr><td>命令</td><td>解释</td></tr>
<tr><td>物理接口配置模式</td><td></td></tr>
<tr><td>{ip|mac|mac-ip} access-group <<i>acl-name</i>> {in|out}[traffic-statistic]
no {ip|mac|mac-ip} access-group <<i>acl-name</i>> {in|out}</td><td>在端口的某个方向上应用一条 access-list；no 操作为删除绑定在端口上的 access-list。</td></tr>
</table>

5. 清空指定接口的包过滤统计信息

命令	解释
特权用户模式	
clear access-group statistic [ethernet<*interface-name*>]	在指定端口清除包过滤统计信息

14.3.2 ACL 配置命令

14.3.2.1 access-list(ip extended)

命令：**access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]**

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [sPort <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [dPort <*dPort*>] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [sPort <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [dPort <*dPort*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

no access-list <*num*>

功能：创建一条匹配特定 IP 协议或所有 IP 协议的数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在，则创建此访问列表。

参数：**<*num*>**为访问表标号，100-199；**<*sIpAddr*>**为源 IP 地址，格式为点分十进制；**<*sMask* >**为源 IP 的反掩码，格式为点分十进制；**<*dIpAddr*>**为目的 IP 地址，格式为点分十进制；**<*dMask*>**为目的 IP 的反掩码，格式为点分十进制，关心的位置 0，忽略的位置 1；**<*igmp-type*>**，igmp 的类型；**<*icmp-type*>**，icmp 的类型；**<*icmp-code*>**，icmp 的协议编号；**<*prec*>**，IP 优先级，0-7；**<*tos*>**，tos 值，0-15；**<*sPort*>**，源端口号，0-65535；**<*dPort*>**，目的端口号，0-65535；**<*time-range-name*>，**时间范围名称。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：当用户第一次指定特定**<*num*>**时，创建此编号的 ACL，之后在此 ACL 中添加表

项。

举例：创建编号为 110 的数字扩展访问列表。拒绝 icmp 报文通过，允许目的地址为 192.168.0.1 目的端口为 32 的 udp 包通过。

Switch(Config)#access-list 110 deny icmp any-source any-destination

Switch(Config)#access-list 110 permit udp any-source host-destination 192.168.0.1 dPort 32

14.3.2.2 access-list(ip standard)

命令：access-list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}

no access-list <*num*>

功能：创建一条数字标准 IP 访问列表，如果已有此访问列表，则增加一条 rule 表项；本命令的 no 操作为删除一条数字标准 IP 访问列表。

参数：<*num*>为访问表标号，1-99；**<*sIpAddr*>**为源 IP 地址，格式为点分十进制；**<*sMask* >**为源 IP 的反掩码，格式为点分十进制。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：当用户第一次指定特定**<*num*>**时，创建此编号的 ACL，之后在此 ACL 中添加表项。

举例：创建一条编号为 20 的数字标准 IP 访问列表，允许源地址为 10.1.1.0/24 的数据包通过，拒绝其余源地址为 10.1.1.0/16 的数据包通过。

Switch(Config)#access-list 20 permit 10.1.1.0 0.0.0.255

Switch(Config)#access-list 20 deny 10.1.1.0 0.0.255.255

14.3.2.3 firewall

命令：firewall { enable | disable}

功能：允许防火墙起作用或禁止防火墙起作用。

参数：enable 表示允许防火墙起作用；**disable** 表示禁止防火墙起作用。

缺省情况：缺省为防火墙不起作用。

命令模式：全局配置模式

使用指南：在允许和禁止防火墙时，都可以设置访问规则。但只有在防火墙起作用时才可以将规则应用至特定端口的特定方向上。使防火墙不起作用后将删除端口上绑定的所有 ACL。

举例：允许防火墙起作用。

Switch(Config)#firewall enable

14.3.2.4 firewall default

命令：firewall default {permit | deny}

功能：设置防火墙默认动作。

参数： permit 表示允许数据包通过；**deny** 表示拒绝数据包通过。

命令模式：全局配置模式

缺省情况：缺省动作为 permit。

使用指南：此命令只影响端口入口方向的 IP
包，其余情况下数据包均可通过交换机。

举例：设置防火墙默认动作为允许数据包通过。

Switch(Config)#firewall default permit

14.3.2.5 ip access extended

命令：**ip access extended <*name*>**

no ip access extended <*name*>

功能：创建一条命名扩展 IP 访问列表；本命令的 no 操作为删除此命名扩展 IP 访问列表（包含所有表项）。

参数：**<*name*>**为访问表标名，字符串长度为 1-16，不允许为纯数字序列。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：第一次以调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例：创建一条名为 tcpFlow 的命名扩展 IP 访问列表。

Switch(Config)#ip access-list extended tcpFlow

14.3.2.6 ip access standard

命令：**ip access standard <*name*>**

no ip access standard <*name*>

功能：创建一条命名标准 IP 访问列表；本命令的 no 操作为删除此命名标准 IP 访问列表（包含所有表项）。

参数：**<*name*>**为访问表标名，字符串长度为 1-16，不允许为纯数字序列。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：第一次以调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例：创建一条名为 ipFlow 的命名标准 IP 访问列表。

Switch(Config)#ip access-list standard ipFlow

14.3.2.7 {ip|mac|mac-ip} access-group

命令：**{ip|mac|mac-ip} access-group <*name*> {in|out}[traffic-statistic]**

no {ip|mac|mac-ip} access-group <*name*> {in|out}

功能：在端口的某个方向上应用一条 access-list，并且根据可选项决定是否对 ACL 规则加上统计计数器；本命令的 no 操作为删除绑定在端口上的 access-list。

参数：**<*name*>，**命名访问表的名字，字符串长度为 1-16。

命令模式：物理端口配置模式

缺省情况：端口的入口和出口方向都没有绑定 ACL。

使用指南：一个端口可以绑定一条入口规则和一条出口规则；ACL 绑定到出口时只能包含 deny 规则，如果是堆叠交换机，则只能在入口绑定 ACL，不能在出口绑定 ACL。

可以绑定**标准的、扩展的和命名的**访问控制列表到三层交换机的**物理端口**上。不能绑定 ACL 到三层接口或汇聚接口上。

基于关心的包头字段 ACL 可以分为三种：
MAC ACL，IP ACL, MAC-IP ACL；某种情况下，当一个数据包匹配六条 ACL 中的多条时，ACL 的过滤动作（permit，deny）会发生冲突。基于结果确定性的考虑，为每一种 ACL 指定了严格的优先级。当过滤动作发生冲突时，可以依据优先级决定包过滤的最终动作,

当绑定 ACL 到端口时，有如下限制：

1. 每个端口入口可以绑定一条 MAC-IP ACL，一条 IP ACL，一条 MAC ACL；
2. 每个端口出口口可以绑定一条 MAC-IP ACL，一条 IP ACL，一条 MAC ACL；
3. 当同时绑定六条 ACL 且数据包同时匹配其中多条 ACL 时，优先关系从高到低如下，如果优先级相同，则先配置的优先级高：
   出口 MAC-IP ACL；
   出口 MAC ACL
   出口 IP ACL
   入口 MAC-IP ACL
   入口 MAC ACL
   入口 IP ACL
4. 出口 ACL 只可以指定 deny 动作；

绑定在接口上的访问控制列表的规则数量必须小于等于 32 条，而且在匹配 TCP 或 UDP 端口号时，只能设置一个端口，不能配置不等于、大于、小于、范围等操作符。
在执行端口绑定命令时，如果规则过于复杂，超出硬件能力，会无法正确绑定，同时输出提示信息。

在软件转发及交换机自身发送数据的情况下，出口规则不起作用。
举例：将名为 aaa 的访问列表绑定到端口的入方向上。
Switch(Config-Ethernet0/0/1)#ip access-group aaa in

14.3.2.8 permit | deny(ip extended)

命令：**[no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]**

[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [sPort <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [dPort <*dPort*>] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [sPort <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [dPort <*dPort*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos

<*tos*>][time-range<*time-range-name*>]
功能：创建一条匹配特定 IP 协议或所有 IP 协议的命名扩展 IP 访问规则；
参数：***<sIpAddr>***为源 IP 地址，格式为点分十进制；***<sMask>***为源 IP 的反掩码，格式为点分十进制；***<dIpAddr>***为目的 IP 地址，格式为点分十进制；***<dMask>***为目的 IP 的反掩码，格式为点分十进制，关心的位置 0，忽略的位置 1；***<igmp-type>***，igmp 的类型，0－255；***<icmp-type>***，icmp 的类型，0－255；***<icmp-code>***，icmp 的协议编号，0－255；***<prec>***，IP 优先级，0－7；***<tos>***，tos 值，0-15；***<sPort>***，源端口号，0-65535；***<dPort>***，目的端口号，0-65535；***<time-range-name>***，时间范围名称。
命令模式：命名扩展 IP 访问列表配置模式
缺省情况：没有配置任何的访问列表。
使用指南：
举例：创建名为 udpFlow 的扩展访问列表。拒绝 igmp 报文通过，允许目的地址为 192.168.0.1 目的端口为 32 的 udp 包通过。
Switch(Config)#ip access-list extended udpFlow
Switch(Config-Ext-Nacl-udpFlow)#access-list 110 deny igmp any-source any-destination
Switch(Config-Ext-Nacl-udpFlow)#access-list 110 permit udp any-source host-destination 192.168.0.1 dPort 32

14.3.2.9 permit | deny(ip standard)

命令：{deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}
no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}
功能：创建一条命名标准 IP 访问规则（rule）；本命令的 no 操作为删除此命名标准 IP 访问规则（rule）。
参数： ***<sIpAddr>***为源 IP 地址，格式为点分十进制；***<sMask>***为源 IP 的反掩码，格式为点分十进制。
命令模式：命名标准 Ip 访问列表配置模式
缺省情况：没有配置任何的访问列表。
使用指南：
举例：允许源地址为 10.1.1.0/24 的数据包通过，拒绝其余源地址为 10.1.1.0/16 的数据包通过。
Switch(Config)# ip access-list standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

14.3.2.10 access-list(mac standard)

命令：access-list <*access-list-number*> {deny|permit} {any-source-mac | {host-source-mac <*host_smac*> } | {<*smac*> <*smac-mask*>} }
no access-list <access-list-number>
功能：定义一条标准数字 MAC ACL 规则，No 命令删除一个标准数字 MAC 访问表规则
参数：***<access-list-number>***访问表号，这是一个从 700 到 799 的十进制号；***deny*** 如果规则匹配，拒绝访问；***permit*** 如果规则匹配，允许访问；***<smac>，<host_smac>*** 源

MAC 地址；**<*smac-mask*>** 源 MAC 地址的
掩码（反掩码）
命令模式：全局配置模式
缺省情况：没有配置任何的访问列表。
使用指南：当用户第一次指定特定**<*num*>**时，创建此编号的 ACL，之后在此 ACL 中添加表项。
举例：允许源 MAC 地址为 00-00-XX-XX-00-01 的数据包通过，拒绝源地址为 00-00-00-XX-00-ab 的数据包通过。
Switch(Config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-01
Switch(Config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-ab

14.3.2.11 access-list(mac extended)

命令：
access-list<*access-list-number*>{deny|permit}{any-source-mac | { host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}{untagged-eth2|tagged-eth2| untagged-802.3 |tagged-802.3}[<*offset1*> <*length1*> <*value1*> [<*offset2*> <*length2*> <*value2*> [<*offset3*> <*length3*> <*value3*> [<*offset4*> <*length4*> <*value4*>]]]]
no access-list <*access-list-number*>
功能：定义一条扩展数字 MAC ACL 规则，No 命令删除一个扩展数字 MAC 访问表规则
参数：
<*access-list-number*>访问表号，这是一个从 1100－1199 的十进制号；***deny*** 如果规则匹配，拒绝访问；***permit*** 如果规则匹配，允许访问；**<*any-source-mac*>**任何源地址；**<*any-destination-mac*>** 任何目的地址；**<*host_smac*>，<*smac*>**源 MAC 地址；**<*smac-mask*>**源 MAC 地址的掩码(反掩码)；**<*host_dmac*>，<*dmac*>** 目的 MAC 地址；**<*dmac-mask*>** 目的 MAC 地址的掩码(反掩码)；**untagged-eth2** 未标记的 ethernet II 包格式；**tagged-eth2** 标记的 ethernet II 包格式；**untagged-802.3** 未标记的 ethernet 802.3 包格式；**tagged-802.3** 标记的 ethernet 802.3 包格式；**Offset(x)** 从包头开始起的偏移量，范围为（12-79），窗口必须从源 MAC 后面开始，从前至后依次配置，并且窗口之间不可重叠，也就是要求：Offset(x＋1) 必须大于或等于 Offset(x)＋len（x)；***Length(x)*** 长度为 1-4，而且 **Offset(x)＋Length(x)必须不大于 80（当前必须不大于 64）**；***Value(x)*** **16 进制数表**示，取值范围：当 **Length(x)** =1 为 0-ff，当 **Length(x)** =2 为 0-ffff，当 **Length(x)** =3 为 0-ffffff，当 **Length(x)** =4 为 0-ffffffff ；

*对于 **Offset(x)**，对不同的数据帧类型，它的取值范围不同：*
对 untagged-eth2 类型帧：<12～51>
对 untagged-802.3 类型帧：<12～55>
对 tagged-eth2 类型帧：<12～59>
对 tagged-802.3 类型帧：<12～63>
命令模式：全局配置配置模式
缺省配置：没有配置任何的访问列表
使用指南：当用户第一次指定特定<*num*>时，创建此编号的 ACL，之后在此 ACL 中添加表项。

举例：允许任意源 MAC 地址任意目的 MAC
地址的 tagged-eth2，且其第 15 16 个字节分别为 0x08 ，0x0 的包通过
Switch(Config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

14.3.2.12 mac access extended

命令：**mac-access-list extended <*name*>**
no mac-access-list extended <*name*>
功能：定义一个命名方式的 MAC ACL 表或进入访问表配置模式，no 命令删除命名方式的 ACL 表。
参数：**<*name*>** 访问表的名字，不包括空格或引号，必须用字母字符开头。长度最大为 16（注：大小写敏感）
命令模式：全局配置模式
缺省配置：没有配置任何的访问列表
使用指南：第一次以调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。
举例：创建一个名字为 mac_acl 的 MAC ACL
Switch(Config)# mac-access-list extended mac_acl
Switch(Config-Mac-Ext-Nacl-mac_acl)#

14.3.2.13 permit | deny(mac extended)

命令：

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype <*protocol*> [<*protocol-mask*>]]

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [untagged-eth2 [ethertype <*protocol*> [protocol-mask]]]

[no]{deny|permit}

{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [untagged-802.3]

[no]{deny|permit}
{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}
[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]
[ethertype<*protocol*> [<*protocol-mask*>]]]

[no]{deny|permit}

{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}
[tagged-802.3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]

功能：定义一条扩展命名 MAC ACL 规则，No 命令删除一个扩展命名 MAC ACL 访问表规则

参数：any-source-mac：任何源 MAC 地址；**any-destination-mac**：任何目的 MAC 地址；***host_smac*** **，*smac***：源 MAC 地址；***smac-mask*** 源 MAC 地址的掩码(反掩码)；***host_dmac*** **，*dmas*** 目的 MAC 地址；***dmac-mask*** 目的 MAC 地址的掩码(反掩码)；***untagged-eth2*：** 未标记的 ethernet II 包格式；***tagged-eth2*：** 标记的 ethernet II 包格式；***untagged-802.3*：** 未标记的 ethernet 802.3 包格式；***tagged-802.3*：** 标记的 ethernet 802.3 包格式；***cos-val*：** cos 值，0-7；***cos-bitmask*：** cos 掩码， 0-7 反掩码且掩码比特连续；***vid-value*：** vlan 号，1-4094；***vid-bitmask*：**vlan 掩码， 0-4095，反掩码且掩码比特连续；***protocol*：** 特定的以太网协议号，1536－65535；***protocol-bitmask*：** 协议掩码，0－65535，反掩码且掩码比特连续

注意：掩码比特连续是指，掩码有效位必须从左第一位开始连续有效，不允许中间插入无效位，例如：一个字节的反掩码形式为：00001111b ；正掩码形式为：11110000；不允许00010011。

命令模式：命名扩展 MAC 访问列表配置模式

缺省配置：没有配置任何的访问列表

使用指南：

14.3.2.14 access-list(mac-ip extended)

命令：

access-list<*num*>{deny|permit}{any-source-mac|
{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac
<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp
{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|
{host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list<*num*>{deny|permit}{any-source-mac|
{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}

{any-destination-mac|{host-destination-mac *<host_dmac>*}|{*<dmac><dmac-mask>*}}igmp {{*<source><source-wildcard>*}|any-source|{host-source*<source-host-ip>*}} {{*<destination><destination-wildcard>*}|any-destination| {host-destination*<destination-host-ip>*}} [*<igmp-type>*] [precedence *<precedence>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list*<num>*{deny|permit}{any-source-mac| {host-source-mac*<host_smac>*}|{*<smac><smac-mask>*}}{any-destination-mac| {host-destination-mac*<host_dmac>*}|{*<dmac><dmac-mask>*}}tcp {{*<source><source-wildcard>*}|any-source| {host-source*<source-host-ip>*}}[s-port*<port1>*] {{*<destination><destination-wildcard>*}|any-destination|{host-destination *<destination-host-ip>*}} [d-port *<port3>*] [ack+fin+psh+rst+urg+syn] [precedence *<precedence>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list*<num>*{deny|permit}{any-source-mac| {host-source-mac*<host_smac>*}|{*<smac><smac-mask>*}}{any-destination-mac| {host-destination-mac*<host_dmac>*}|{*<dmac><dmac-mask>*}}udp {{*<source><source-wildcard>*}|any-source| {host-source*<source-host-ip>*}}[s-port*<port1>*] {{*<destination><destination-wildcard>*}|any-destination| {host-destination*<destination-host-ip>*}}[d-port*<port3>*] [precedence *<precedence>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list*<num>*{deny|permit}{any-source-mac| {host-source-mac*<host_smac>*}|{*<smac><smac-mask>*}} {any-destination-mac|{host-destination-mac *<host_dmac>*}|{*<dmac><dmac-mask>*}} {eigrp|gre|igrp|ip|ipinip|ospf|{*<protocol-num>*}} {{*<source><source-wildcard>*}|any-source|{host-source*<source-host-ip>*}} {{*<destination><destination-wildcard>*}|any-destination| {host-destination*<destination-host-ip>*}} [precedence *<precedence>*] [tos *<tos>*][time-range*<time-range-name>*]

功能：定义一条扩展数字 MAC-IP ACL 规则，No 命令删除一个扩展数字 MAC-IP ACL 访问表规则

参数： ***access-list-number*** 访问表号。这是一个从 3100－3199 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；**any-source-mac**：任何源 MAC 地址；**any-destination-mac**：任何目的 MAC 地址；**host_smac** ，**smac**：源 MAC 地址；**smac-mask**：源 MAC 地址的掩码(反掩码)；**host_dmac** ，**dmas** 目的 MAC 地址；**dmac-mask** 目的 MAC 地址的掩码(反掩码)；**protocol** 名字或 IP 协议的号。它可以是关键字 eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, 也可以是表 IP 协议号的 0 到 255 的一个整数。为了匹配任何 Internet 协议（包括 ICMP，TCP 和 UDP）使用关键字 ip。；**source-host-ip, source** 包发送的源网络或源主机号。32 位二进制数，点分十进制表示。；

host-source:表示地址是源主机 IP 地址，否则是网络 IP 地址。；**source-wildcard**:源 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**destination-host-ip**，**destination** 包发送时要去往的目的网络或主机号。32 位二进制数，点分十进制表示；**host-source**:表示地址是目的主机 IP 地址，否则是网络 IP 地址；**destination-wildcard**：目的 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**s-port**(可选)：表示要匹配 TCP/UDP 源端口；**port1**(可选)**:** TCP/UDP 源端口号值，端口号是一个 0 到 65535 的数字；**d-port**(可选)：表示要匹配 TCP/UDP 目的端口；**port3**(可选)：TCP/UDP 目的端口号值，端口号是一个 0 到 65535 的数字；**[ack] [fin] [psh] [rst] [urg] [syn]**，(可选) 只对 TCP 协议，可选多个标志位，当 TCP 数据报**[ack] [fin] [psh] [rst] [urg] [syn]**的相应位设置时，即初始化 TCP 数据报以形成一个连接时出现匹配；**precedence** (可选) 包可由优先级过滤， 为 0 到 7 的数字；**tos** (可选)包可由服务级类型过滤，为 0 到 15 的数字；**icmp-type** (可选) ICMP 包可由 ICMP 报文类型过滤。类型是数字 0 到 255；**icmp-code** (可选) ICMP 包可由 ICMP 报文码过滤。该代码是数字 0 到 255；**igmp-type** (可选) IGMP 包可由 IGMP 报文类型或报文名过滤。类型是数字 0 到 15；**<*time-range-name*>**，时间范围名称。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：当用户第一次指定特定**<*num*>**时，创建此编号的 ACL，之后在此 ACL 中添加表项。

举例：允许源 MAC 为 00-12-34-45-XX-XX，任意目的 MAC 地址，源 IP 地址为：100.1.1.0 0.255.255.255，任意目的 IP 地址，且源端口是 100，目的端口是 40000 的 TCP 报文通过

Switch(Config)# access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-port 40000

14.3.2.15 mac-ip access extended

命令：**mac-ip-access-list extended <*name*>**

no mac-ip-access-list extended <*name*>

功能：定义一个命名方式的 MAC-IP ACL 表或进入访问表配置模式，no 命令删除命名方式的 ACL 表。

参数：***name*** 访问表的名字，不包括空格或引号，必须用字母字符开头。长度最大为 16（注：大小写敏感）

命令模式：全局配置模式

缺省情况：没有命名的 MAC-IP 访问表

使用指南：第一次以调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例：

创建一个名字为 macip_acl 的 MAC-IP ACL

Switch(Config)# mac-ip-access-list extended macip_acl

Switch(Config-MacIp-Ext-Nacl-macip_acl)#

14.3.2.16 permit | deny(mac-ip extended)

命令：

[no] {deny|permit}

{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}
{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}
icmp{{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|{host-destination
<destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>]
[tos <tos>][time-range<time-range-name>]

[no]{deny|permit}

{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}
{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}
igmp{{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|{host-destination
<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]

[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|
{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}}tcp{{<source><source-wildcard>}|any-source|
{host-source<source-host-ip>}}[s-port<port1>]{{<destination>
<destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}}
[d-port <port3>] [ack＋fin＋psh＋rst＋urg＋syn] [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]

[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac>
<smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}}udp{{<source><source-wildcard>}|any-source|
{host-source<source-host-ip>}}[s-port<port1>]{{<destination>
<destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}}
[d-port <port3>] [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]

[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac>
<smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}}
{{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|{host-destination
<destination-host-ip>}} [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]

功能：定义一条扩展命名 MAC-IP ACL 规则，

No 命令删除一个扩展数字 MAC-IP ACL 访问表规则。

参数：***access-list-number*** 访问表号。这是一个从 3100－3199 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；**any-source-mac**：任何源 MAC 地址；**any-destination-mac**：任何目的 MAC 地址；**host_smac ，smac**：源 MAC 地址；**smac-mask**：源 MAC 地址的掩码(反掩码)；**host_dmac ，dmas** 目的 MAC 地址；**dmac-mask** 目的 MAC 地址的掩码(反掩码)；**protocol** 名字或 IP 协议的号。它可以是关键字 eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, 也可以是表 IP 协议号的 0 到 255 的一个整数。为了匹配任何 Internet 协议（包括 ICMP，TCP 和 UDP）使用关键字 ip。；**source-host-ip, source** 包发送的源网络或源主机号。32 位二进制数，点分十进制表示。；**host-source**:表示地址是源主机 IP 地址，否则是网络 IP 地址。；**source-wildcard**:源 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**destination-host-ip，destination** 包发送时要去往的目的网络或主机号。32 位二进制数，点分十进制表示；**host-source**:表示地址是目的主机 IP 地址，否则是网络 IP 地址；**destination-wildcard**：目的 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**s-port**(可选)：表示要匹配 TCP/UDP 源端口；**port1**(可选)**:** TCP/UDP 源端口号值，端口号是一个 0 到 65535 的数字；**d-port**(可选)：表示要匹配 TCP/UDP 目的端口；**port3**(可选)：TCP/UDP 目的端口号值，端口号是一个 0 到 65535 的数字；**[ack] [fin] [psh] [rst] [urg] [syn]** (可选) 只对 TCP 协议，可选多个标志位，当 TCP 数据报[ack] [fin] [psh] [rst] [urg] [syn]的相应位设置时，即初始化 TCP 数据报以形成一个连接时出现匹配；**precedence** (可选) 包可由优先级过滤， 为 0 到 7 的数字；**tos** (可选)包可由服务级类型过滤，为 0 到 15 的数字；**icmp-type** (可选) ICMP 包可由 ICMP 报文类型过滤。类型是数字 0 到 255；**icmp-code** (可选) ICMP 包可由 ICMP 报文码过滤。该代码是数字 0 到 255；**igmp-type** (可选) IGMP 包可由 IGMP 报文类型或报文名过滤。类型是数字 0 到 15；***<time-range-name>，*** 时间范围名称。

命令模式：命名扩展 MAC-IP 访问列表配置模式

缺省情况：没有配置任何的访问列表。

使用指南：

举例：拒绝任意源 MAC 地址及目的 MAC 地址，任意源 IP 地址及目的 IP 地址，且源端口是 100，目的端口是 40000 的 UDP 报文通过

Switch(Config)# access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000

14.3.2.17 time-range

命令：**[no] time-range <*time_range_name*>**

功能： 创建一个名为 **time_range_name** 的时间范围名，并同时进入时间范围模式。

参数：***time_range_name*** 时间范围名字，必须用字母字符开头，名字最大长度为 16 个字符。

命令模式：全局配置模式

缺省情况：没有时间范围配置

使用指南：

举例：创建一个名为 dc_timer 的时间范围

Switch(config)#Timer-range dc_timer

14.3.2.18 absolute-periodic/periodic

命令：
[no] absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <end_time>
[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily| weekdays | weekend} <start_time> to <end_time>
功能： 定义一周内的各种不同要求的时间范围，每周都循环这个时间。
参数：
Friday Friday(星期五)
Monday Monday (星期一)
Saturday Saturday (星期六)
Sunday Sunday (星期日)
Thursday Thursday （星期四）
Tuesday Tuesday (星期二)
Wednesday Wednesday (星期三)
daily Every day of the week （每天）
weekdays Monday thru Friday （星期一到星期五）
weekend Saturday and Sunday （星期六到星期日）
start_time 开始时间点，hh:mm (小时：分钟)
end_time 结束时间点，hh:mm (小时：分钟)
注：time-range 轮询时间是 1 分钟一次，所以时间的误差<=1 分钟。
命令模式：时间范围模式
缺省情况：没有时间范围配置
使用指南：周期性的时间和日期，周期是定义每周的 1～6 和周日的具体时间段，可以同时配置多个周期性时段，它们之间是"或"的关系。它的形式是：
day1 hh:mm:ss To day2 hh:mm:ss 或者
{[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss
举例：使能在 Tuesday 到 Saturday 内的 9:15:30 到 12:30:00 时间段内配置生效
Switch(Config)#time-range dc_timer
Switch(Config-Time-Range)# absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00
使能在 Monday、Wednesday、Friday 和 Sunday 四天内的 14:30:00 到 16:45:00 时间段配置生效
Switch#(Config-Time-Range) periodic Monday+Wednesday+Friday+Sunday 14:30:00 to 16:45:00

14.3.2.19 absolute start

命令：**[no]absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]**
功能：定义一个绝对时间段,这个时间段是根据本设备的时钟运行。

参数：***start_time*** ：开始时间点，hh:mm (小
时：分钟)

end_time ： 结束时间点，hh:mm (小时：分钟)

start_data ：开始日期，格式是，YYYY.MM.DD（年.月.日）

end_data ： 结束日期，格式是，YYYY.MM.DD（年.月.日）

注：time-range 轮询时间是 1 分钟一次，所以时间的误差<=1 分钟。

命令模式：时间范围模式

缺省情况：没有时间范围配置

使用指南：绝对时间及日期，指定具体开始的年，月，日，小时，分钟，不能配置多个绝对时间及日期，重复配置时，后配置的覆盖以前配置的绝对时间及日期。

举例：使能在 2004.10.1 到 2005.1.26 内从 6:00:00 到 13:30:00 配置生效

Switch(config)#Time-range dcn_timer
Switch#(Config-Time-Range) absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

14.3.2.20 clear access-group statistic

命令：**clear access-group statistic [ethernet<*interface-name*>]**

功能：清空指定接口的包过滤统计信息

参数：**<*interface-name*>**：接口名称

命令模式：全局配置模式

缺省情况：无

举例：清空接口 E0/0/1 的包过滤统计信息

Switch(config)#clear access-group statistic e0/0/1

14.4 ACL 举例

案例 1：

用户有如下配置需求：交换机的 10 端口连接 10.0.0.0/24 网段，管理员不希望用户使用 ftp。

配置更改：

1. 创建相应的 ACL
2. 配置包过滤功能
3. 绑定 ACL 到端口

配置步骤如下：

Switch(Config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#ip access-group 110 in
Switch(Config-Ethernet0/0/10)#ex
Switch(Config)#ex

配置结果：

Switch#show firewall

Firewall Status: Enable.
Firewall Default Rule: Permit.
Switch#show access-lists
access-list 110(used 1 time(s))
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 0/0/10
interface name:Ethernet0/0/10
the ingress acl use in firewall is 110.

案例 2：

用户有如下配置需求：交换机的 10 端口连接的网段的 MAC 地址是 00-12-11-23-XX-XX，并且不允许 802.3 的数据报文发出。

配置更改：

1、 创建相应的 MAC ACL
2、 配置包过滤功能
3、 绑定 ACL 到端口

配置步骤如下：

Switch(Config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any untagged-802.3
Switch(Config)# access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802.3
Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#ip access-group 1100 in
Switch(Config-Ethernet0/0/10)#ex
Switch(Config)#ex

配置结果：

Switch#show firewall
fire wall is enable
the default action of fire wall is permit

Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac untagged-802.3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac tagged-802.3
Switch #show access-group
interface name:Ethernet0/0/10
MAC Ingress access-list used is 1100.

案例 3：

用户有如下配置需求：交换机的 10 端口连接的网段的 MAC 地址是 00-12-11-23-XX-XX，并且 IP 为 10.0.0.0/24 网段，管理员不希望用户使用 ftp，也不允许外网 ping 此网段的任何一台主机。

配置更改：

1、 创建相应的 ACL
2、 配置包过滤功能
3、 绑定 ACL 到端口

配置步骤如下：

```
Switch(Config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(Config)#access-list 3120 deny any 00-12-11-23-00-00 00-00-00-00-FF-FF icmp any-source 10.0.0.0 0.0.0.255

Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#mac-ip access-group 3110 in
Switch(Config-Ethernet0/0/10)#mac-ip access-group 3120 out
Switch(Config-Ethernet0/0/10)#ex
Switch(Config)#ex
```

配置结果：

```
Switch#show firewall
  fire wall is enable
  the default action of fire wall is permit

Switch#show access-lists
access-list 3120(used 1 time(s))
  access-list 3120 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-FF-FF icmp any-source 10.0.0.0 0.0.0.255

access-list 3110(used 1 time(s))
    access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch #show access-group
interface name:Ethernet0/0/10
    MAC-IP Ingress access-list used is 3110.
    MAC-IP Egress access-list used is 3120.
```

14.5 ACL 排错帮助

14.5.1 ACL 调试和监测命令

14.5.1.1 show access-lists

命令：show access-lists [<*num*>|<*acl-name*>]
功能：显示配置的访问控制列表。
参数：*<acl-name>*，特定的访问控制列表命名字符串；***<num>*，**特定的访问控制列表的编号。
缺省情况：无。
命令模式：特权模式
使用指南：不指定访问控制列表的名字时，会显示所有的访问控制列表；used x time（s）表明了此 ACL 被引用的次数。
举例：

Switch#show access-lists
access-list 10(used 0 time(s))
    access-list 10 deny any-source

access-list 100(used 1 time(s))
    access-list 100 deny ip any-source any-destination
    access-list 100 deny tcp any-source any-destination

access-list 1100(used 0 time(s))
    access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

access-list 3100(used 0 time(s))
    access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000

显示内容	解释
access-list 10(used 1 time(s))	数字 ACL10，被引用 0 次
access-list 10 deny any-source	拒绝所有 IP 数据包通过
access-list 100(used 1 time(s))	数字 ACL100，被引用 1 次
access-list 100 deny ip any-source any-destination	拒绝任意源 IP 地址及目的 IP 地址的 IP 包通过
access-list 100 deny tcp any-source any-destination	拒绝任意源 IP 地址及目的 IP 地址的 TCP 包通过
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	允许任意源MAC地址任意目的MAC地址的tagged-eth2，且其第 15 16 个字节分别为 0x08 ，0x0 的包通过
access-list 3100 permit any-source-mac	拒绝任意源 MAC 地址及目的 MAC 地址，任

any-destination-mac udp any-source s-port 100 any-destination d-port 40000	意源 IP 地址及目的 IP 地址，且源端口是 100，目的端口是 40000 的 UDP 报文通过

14.5.1.2 show access-group

命令：**show access-group [interface [Ethernet] <*name*>]**
功能：显示端口上 ACL 绑定情况。
参数：**<*name*>**，接口名。
缺省情况：无。
命令模式：特权模式
使用指南：不指定接口名时，会显示所有端口上绑定的 ACL。
举例：

```
Switch#show access-group
interface name:Ethernet0/0/2
    the ingress acl use in firewall is 111,packet(s) number is 10.
    the egress acl use in firewall is 100,packet(s) number is 10.
interface name:Ethernet0/0/1
    the ingress acl use in firewall is 10,packet(s) number is 10.
```

显示内容	解释
interface name:Ethernet0/0/2	端口 Ethernet0/0/2 的绑定情况
the ingress acl use in firewall is 111.	端口 Ethernet0/0/2 入口方向绑定了编号 111 的数字扩展 ACL
the egress acl use in firewall is 100.	端口 Ethernet0/0/2 出口方向绑定了编号 100 的数字扩展 ACL
interface name:Ethernet0/0/1	端口 Ethernet0/0/1 的绑定情况
the ingress acl use in firewall is 10.	端口 Ethernet0/0/1 入口方向绑定了编号 10 的数字标准 ACL
packet(s) number is 10	统计到匹配此 ACL 规则的数据包数

14.5.1.3 show firewall

命令：**show firewall**
功能：显示包过滤功能配置信息。
参数：无。
缺省情况：无。
命令模式：特权模式
使用指南：
举例：

```
Switch#show firewall
fire wall is enable
```

the default action of fire wall is permit

显示内容	解释
fire wall is enable	包过滤功能打开
the default action of firewall is permit	包过滤默认动作为 permit

14.5.1.4 show time-range

命令：show time-range<*word*>
功能：显示时间范围功能配置信息。
参数：*word* 指定要显示的 time-range 的名字
缺省情况：无。
命令模式：特权模式
使用指南： 不指定 time-range 的名字时，显示所有的 time-range
举例：
Switch#show time-range
time-range timer1 (inactive)
    absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (active)
    absolute-periodic Monday 0:0:0 to Friday 23:59:59

14.5.2 ACL 排错帮助

- 对 ACL 中的表项的检查是自上而下的，只要匹配一条表项，对此 ACL 的检查就马上结束。
- 端口特定方向上没有绑定 ACL 或没有任何 ACL 表项匹配时，才会使用默认规则。
- 每个端口入口可以绑定一条 MAC-IP ACL，一条 IP ACL，一条 MAC ACL；
- 每个端口出口口可以绑定一条 MAC-IP ACL，一条 IP ACL，一条 MAC ACL；
- 当同时绑定六条 ACL 且数据包同时匹配其中多条 ACL 时，优先关系从高到低如下，如果优先级相同，则先配置的优先级高：
  出口 MAC-IP ACL；
  出口 MAC ACL
  出口 IP ACL
  入口 MAC-IP ACL
  入口 MAC ACL
  入口 IP ACL
- 当一条 ACL 被绑定到端口出口方向时，只能包含 deny 表项。
- 只在 MASTER 交换机上的接口支持绑定访问控制列表。
- 端口可以成功绑定的 ACL 数目取决于已绑定的 ACL 的内容以及硬件资源限制。
- 如果 access-list 中包括过滤信息相同但动作矛盾的规则，则其无法绑定到端口并将有报错提示。例如同时配置 permit tcp any-source any-destination 及 deny tcp any-source any-destination。
- 可以配置 ACL 拒绝某些 ICMP 报文通过以防止“冲击波”等病毒攻击。

☞ 对于堆叠交换机和 DCS-3950S，则只能在入口绑定 ACL，不能在出口绑定 ACL。

第15章Por t Channel 配置

15.1 Port Channel 介绍介绍

在介绍 Port Channel 之前，先介绍一下 Port Group 的概念：Port Group 是配置层面上的一个物理端口组，配置到 Port Group 里面的物理端口才可以参加链路汇聚，并成为 Port Channel 里的某个成员端口。在逻辑上，Port Group 并不是一个端口，而是一个端口序列。加入 Port Group 中的物理端口满足某种条件时进行端口汇聚，形成一个 Port Channel，这个 Port Channel 具备了逻辑端口的属性，才真正成为一个独立的逻辑端口。端口汇聚是一种逻辑上的抽象过程，将一组具备相同属性的端口序列，抽象成一个逻辑端口。Port Channel 是一组物理端口的集合体，在逻辑上被当作一个物理端口。对用户来讲，完全可以将这个 Port Channel 当作一个端口使用，因此不仅能增加网络的带宽，还能提供链路的备份功能。端口汇聚功能通常在交换机连接路由器、主机或者其他交换机时使用。

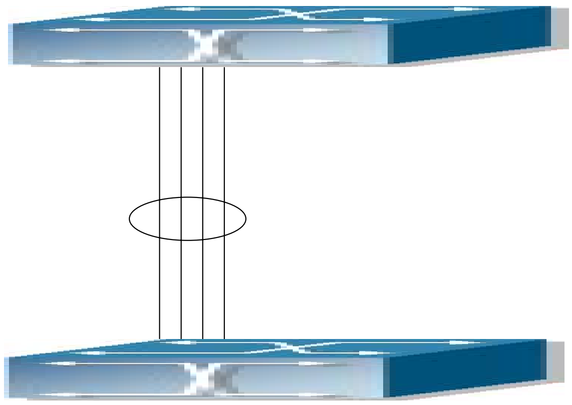


图 15-1 端口聚合示意图

如上图中显示交换机 S1 的 1-4 号端口汇聚成一个 Port Channel，该 Port Channel 的带宽为 4 个端口带宽的总和。而 S1 如果有流量要经过 Port Channel 传输到 S2，S1 的 Port Channel 将根据流量的源 MAC 地址及目的 MAC 地址的最低位进行流量分配运算，根据运算结果决定由 Port Channel 中的某一成员端口承担该流量。当 Port Channel 中的一个端口连接失败，原应该由该端口承担的流量将再次通过流量分配算法分配给其他连接正常的端口分担。流量分配算法由交换机的硬件决定的。

神州数码交换机提供了两种配置端口汇聚的方法：手工生成 Port Channel、LACP（Link Aggregation Control Protocol）动态生成 Port Channel。只有双工模式为全双工模式的端口才能进行端口汇聚。

为使 Port Channel 正常工作，本交换机 Port Channel 的成员端口必须具备以下相同的属性：

- 端口均为全双工模式；
- 端口速率相同；

- ☞ 端口的类型必须一样，比如同为以太口或同为光纤口；
- ☞ 端口同为 Access 端口并且属于同一个 VLAN 或同为 Trunk 端口；
- ☞ 如果端口为 Trunk 端口，则其 Allowed VLAN 和 Native VLAN 属性也应该相同。

当交换机通过手工方式配置 Port Channel 或 LACP 方式动态生成 Port Channel，系统将自动选举出 Port Channel 中端口号最小的端口作为 Port Channel 的主端口（Master Port）。若交换机打开 Spanning-tree 功能，Spanning-tree 视 Port Channel 为一个逻辑端口，并且由主端口发送 BPDU 帧。

另外，端口汇聚功能的实现与交换机所使用的硬件有密切关系，神州数码交换机支持任意两个交换机物理端口的汇聚，最大组数为 6 个，组内最多的端口数为 8 个。

汇聚端口一旦汇聚成功就可以把它当成一个普通的端口使用，在交换机中还建立了汇聚接口配置模式，与 vlan 和物理接口配置模式一样，用户能在汇聚接口配置模式下对汇聚端口进行相关的配置。

15.2 Port Channel 配置

15.2.1 Port Channel 配置任务序列

1. 全局模式下建立一个port group
2. 分别在端口模式下将这些端口加入指定的group
3. 进入port-channel配置模式

命令	解释
全局配置模式	
port-group ***<port-group-number>*** **[load-balance { src-mac|dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}]** **no port-group <port-group-number> [load-balance]**	创建或删除一个 port group，并且设置该组的流量分担方式。

1.创建 port group

命令	解释
接口配置模式	
port-group ***<port-group-number>*** **mode {active|passive|on}** **no port-group** ***<port-group-number>***	把端口加入 port group，并设置模式。

2.把物理端口加入 port group

3.进入 port-channel 配置模式

命令	解释

全局配置模式	
interface port-channel <*port-channel-number*>	进入 port-channel 配置模式。

15.2.2 Port Channel 配置命令

15.2.2.1 port-group

命令： **port-group <*port-group-number*> [load-balance { src-mac|dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}]**

no port-group <port-group-number> [load-balance]

功能： 新建一个 port group，并且设置该组的流量分担方式。如果没有指定流量分担方式则为设置默认的流量分担方式。该命令的 no 操作为删除该 group 或者恢复该组流量分担的默认值，敲入 load-balance 表示恢复默认流量分担，否则为删除该组。

参数：<*port-group-number*> 为 Port Channel 的组号，范围为 1～16，如果已经存在该组号则会报错。**dst-mac** 根据目的 MAC 进行流量分担；**src-mac** 根据源 MAC 地址进行流量分担；**dst-src-mac** 根据目的 MAC 和源 MAC 进行流量分担；**dst-ip** 根据目的 IP 地址进行流量分担；**src-ip** 根据源 IP 地址进行流量分担；**dst-src-ip** 根据目的 IP 和源 IP 进行流量分担。如果是修改流量分担方式，并且该 port-group 已经形成一个 port-channel，则这次修改的流量分担方式只有在下次再次汇聚时才会生效。

缺省情况：缺省交换机端口不属于 Port Channel，不启动 LACP 协议

命令模式：交换机全局配置模式

举例：新建一个 port group，并且采用默认的流量分担方式

Switch(Config)#port-group 1

删除一个 port group

Switch(Config)#no port-group 1

15.2.2.2 port-group mode

命令：port-group <*port-group-number*> mode {active|passive|on}

no port-group <*port-group-number*>

功能：将物理端口加入 Port Channel，该命令的 no 操作为将端口从 Port Channel 中去除

参数：<*port-group-number*> 为 Port Channel 的组号，范围为 1～16；**active（0）** 启动端口的 LACP 协议，并设置为 Active 模式；**passive（1）** 启动端口的 LACP 协议，并且设置为 Passive 模式；**on（2）** 强制端口加入 Port Channel，不启动 LACP 协议。

命令模式：交换机接口配置模式

缺省情况：缺省交换机端口不属于 Port Channel，不启动 LACP 协议

使用指南：如果不存在该组则会先建立该组，然后再将端口加到组中。在一个 port-group 中所有的端口加入的模式必须一样，以第一个加入该组的端口模式为准。端口以 on 模式加入一个组是强制性的，所谓强制性的表示本端交换机端口汇聚不依赖对端的信息，只要在组中有 2 个以上的端口，并且这些端口的 vlan 信息都一致则组中的端口就能汇聚成功。端口

以 active 和 passive 方式加入一个组是运行 lacp 协议的，但两端必须有一个组中的端口是以 active 方式加入的，如果两端都是 passive，端口永远都无法汇聚起来。

举例：在 Ethernet0/0/1 端口模式下，将本端口以 active 模式加入 port-group 1

Switch(Config-Ethernet0/0/1)#port-group 1 mode active

15.2.2.3 interface port-channel

命令：interface port-channel <*port-channel-number*>

功能：进入汇聚接口配置模式

命令模式：全局配置模式

缺省情况：

使用指南：进入汇聚端口模式下配置时，如果是对 gvrp,spanningtree 模块做配置则对汇聚端口生效，如果汇聚端口不存在，也就是说在端口没有汇聚起来时先提示错误信息，记录该用户配置操作，当端口真正汇聚起来以后恢复用户刚才对未形成汇聚端口的配置动作，注意只能恢复一次，如果因为某种原因汇聚组被拆散然后又汇聚起来，用户一开始的配置不能被恢复。如果是对其他模块做配置，比如做 shutdown 配置，则是对该 port-channel 对应的 port-group 中的所有成员端口生效，起到一个群配的作用。

举例：进入 port-channel1 配置模式

Switch(Config)#interface port-channel 1

Switch(Config-If-Port-Channel1)#

15.3 Port Channel 举例

案例 1：以 LACP 方式配置 Port Channel。

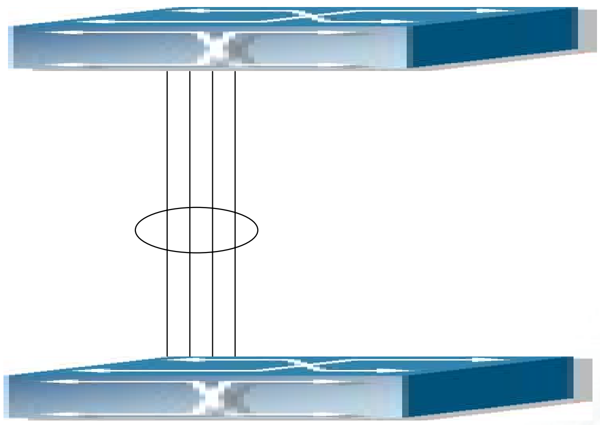


图 15-2 以 LACP 方式配置 Port Channel

在下面说明中都用 Switch 来表示神州数码交换机。

如图所示，交换机 Switch1 上的 1，2，3 端口都是 access 口，并且都属于 vlan 1，将这三个端口以 active 方式加入 group 1，Switch2 上 6，8，9 端口为 trunk 口，并且是 allow all，

将这三个端口以 passive 方式加入 group 2，
将以上对应端口分别用网线相连。

配置步骤如下：

```
Switch1#config
Switch1 (Config)#interface eth 0/0/1-3
Switch1 (Config-Port-Range)#port-group 1 mode active
Switch1 (Config-Port-Range)#exit
Switch1 (Config)#interface port-channel 1
Switch1 (Config-If-Port-Channel1)#

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 0/0/6
Switch2 (Config-Ethernet0/0/6)#port-group 2 mode passive
Switch2 (Config-Ethernet0/0/6)#exit
Switch2 (Config)# interface eth 0/0/8-9
Switch2 (Config-Port-Range)#port-group 2 mode passive
Switch2 (Config-Port-Range)#exit
Switch2 (Config)#interface port-channel 2
Switch2 (Config-If-Port-Channel2)#
```

配置结果：

过一段时间后，shell 提示端口汇聚成功，此时 Switch1 的端口 1，2，3 汇聚成一个汇聚端口，汇聚端口名为 Port-Channel1，Switch2 的端口 6，8，9 汇聚成一个汇聚端口，汇聚端口名为 Port-Channel2，并且都可以进入汇聚接口配置模式进行配置。

案例 2：以 ON 方式配置 Port Channel。

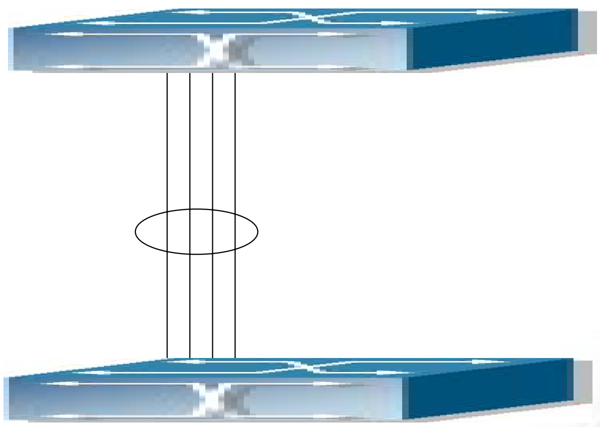


图 15-3 以 ON 方式配置 Port Channel

如图所示，交换机 Switch1 上的 1，2，3 端口都是 access 口，并且都属于 vlan 1，将这三个端口以 on 方式加入 group 1，在 Switch2 上 6，8，9 端口为 trunk 口，并且是 allow all，

将这三个端口以 on 方式加入 group 2。

配置步骤如下：

Switch1#config
Switch1 (Config)#interface eth 0/0/1
Switch1 (Config-Ethernet0/0/1)# port-group 1 mode on
Switch1 (Config-Ethernet0/0/1)#exit
Switch1 (Config)#interface eth 0/0/2
Switch1 (Config-Ethernet0/0/2)# port-group 1 mode on
Switch1 (Config-Ethernet0/0/2)#exit
Switch1 (Config)#interface eth 0/0/3
Switch1 (Config-Ethernet0/0/3)# port-group 1 mode on
Switch1 (Config-Ethernet0/0/3)#exit

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 0/0/6
Switch2 (Config-Ethernet0/0/6)#port-group 2 mode on
Switch2 (Config-Ethernet0/0/6)#exit
Switch2 (Config)# interface eth 0/0/8-9
Switch2 (Config-Port-Range)#port-group 2 mode on
Switch2 (Config-Port-Range)#exit

配置结果：

将交换机 Switch1 上的 1，2，3 三个端口依次加入 port-group1 后我们可以看到，以 on 方式加入一个组完全是强制性的，两端的交换机并不会通过交换 LACP PDU 来完成汇聚，汇聚也是触发式的，当敲入将 2 号端口加入 port-group1 的命令时，1 和 2 马上汇聚在一起形成 port-channel1，当将 3 号端口加入 port-group1 时，1 和 2 汇聚成的 port-channel1 被拆散，马上 1，2，3 三个端口又重新汇聚成 port-channel1（需要说明的是，当有一个新的端口要加入已经汇聚成功的组时，必须先拆散原先的组，然后再能汇聚成一个新的组）。结果是 Switch1 和 Switch2 上的三个端口都以 ON 模式汇聚起来，各自形成一个汇聚端口。

15.4 Port Channel 排错帮助

15.4.1 监测和调试命令

15.4.1.1 show port-group

命令：**show port-group [<*port-group-number*>] {brief | detail | load-balance | port | port-channel}**

参数：**<*port-group-number*>** 要显示的 Port Channel 的组号，范围为 1～16；brief 显示

摘要信息；detail 显示详细信息；load-balance
显示流量分担信息； port 显示成员端口信息； port-channel 显示汇聚端口信息

命令模式：特权用户配置模式

使用指南：如果没有指定 port-group-number 则表示显示所有 port-group 的信息。

举例：将端口 0/0/1 和 0/0/2 加入 port-group 1 中

1. 显示交换机的 port-group 1 的摘要信息。

Switch#show port-group 1 brief
Port-group number : 1
Number of ports in group : 2   Maxports = 8
Number of port-channels : 0   Max port-channels : 1

显示内容	解释
Number of ports in group	在 port-group 中的端口数
Maxports	组中最大允许的端口数
Number of port-channels	是否已经汇聚成一个汇聚端口
Max port-channels	Port-group 所能形成的最大汇聚端口数

2. 显示交换机的 port-group 1 的详细信息。

Switch# show port-group 1 detail
Sorted by the ports in the group 1:
----
port Ethernet0/0/1 :
both of the port and the agg attributes are not equal
the general information of the port are as follows:
portnumber: 1   actor_port_agg_id:0   partner_oper_sys:0x000000000000
partner_oper_key: 0x0001   actor_oper_port_key: 0x0101
mode of the port: ACTIVE   lacp_aware: enable
begin: FALSE   port_enabled: FALSE   lacp_ena: FALSE   ready_n: TRUE

the attributes of the port are as follows:
mac_type: ETH_TYPE   speed_type: ETH_SPEED_10M
duplex_type: FULL   port_type: ACCESS

the machine state and port state of the port are as the follow
mux_state: DETCH   rcvm_state: P_DIS   prm_state: NO_PER
actor_oper_port_state : L_A___F_
partner_oper_port_state: _TA___F_

port Ethernet0/0/2 :
both of the port and the agg attributes are not equal
the general information of the port are as follows:
portnumber: 2   actor_port_agg_id:0   partner_oper_sys:0x000000000000
partner_oper_key: 0x0002   actor_oper_port_key: 0x0102
mode of the port: ACTIVE   lacp_aware: enable

begin: FALSE   port_enabled: FALSE
lacp_ena: TRUE   ready_n: TRUE

the attributes of the port are as follows:
mac_type: ETH_TYPE   speed_type: ETH_SPEED_100M
duplex_type: FULL   port_type: ACCESS

the machine state and port state of the port are as the follow
mux_state: DETCH   rcvm_state: P_DIS   prm_state: NO_PER
actor_oper_port_state   :   L_A___F_
partner_oper_port_state: _TA___F_

显示内容	解释
portnumber	端口号
actor_port_agg_id	该端口加入的 channel 号，如果由于端口参数与 channel 的参数不一致导致该端口不能进入 channel，显示为 0
partner_oper_sys	对端的 system ID
partner_oper_key	对端的 operational key
actor_oper_port_key	本端的 operational key
mode of the port	端口加入组的模式
mac_type	端口的类型，分标准以太网口和光纤分布式数据接口
speed_type	端口的 speed 类型，分 10M 和 100M 口
duplex_type	端口的双工类型，分全双工和半双工
port_type	端口的 vlan 属性，分 access 口和 trunk 口
mux_state	端口绑定状态机的状态
rcvm_state	端口收包状态机的状态
prm_state	端口发包状态机的状态

3. 显示交换机的 port-group 1 的显示流量分担信息。
Switch# show port-group 1 load-balance
The loadbalance of the group 1 based on src MAC address.

4．显示交换机的 port-group 1 的成员端口信息。
Switch# show port-group 1 port
Sorted by the ports in the group 1 :
----
the portnum is 1
port Ethernet0/0/1 related information:

Actor part
                    Administrative   Operational
port number   1
port priority   0x8000
aggregator id   0
port key   0x0100   0x0101

```
port state
LACP activety              .                    1
LACP timeout                .                    .
Aggregation                1                    1
Synchronization            .                    .
Collecting                 .                    .
Distributing               .                    .
Defaulted                  1                    1
Expired                    .                    .


Partner part
                     Administrative        Operational
system                   000000-000000        000000-000000
system priority        0x8000                0x8000
key                      0x0001                0x0001
port number                1                     1
port priority          0x8000                0x8000
port state
LACP activety              .                     .
LACP timeout                1                     1
Aggregation                1                     1
Synchronization            .                     .
Collecting                 .                     .
Distributing               .                     .
Defaulted                  1                     1
Expired                    .                     .

Selected                                  Unselected
```

显示内容	解释
portnumber	端口号
port priority	端口优先级
system	system ID
system priority	System 优先级
LACP activety	端口是否以 active 模式加入组，如果是置 1
LACP timeout	端口超时方式，如果是短超时置 1
Aggregation	端口是否可汇聚，如果为 0 表示该端口为独立端口，不允许参与汇聚
Synchronization	端口是否与对端同步
Collecting	端口绑定状态机状态是否到达 collecting 状态
Distributing	端口绑定状态机状态是否到达 distributing 状态
Defaulted	本端端口是否使用默认的对端参数
Expired	端口收包状态机的状态是否处在 expire 状态
Selected	端口是否已被选择

5．显示交换机的 port-group 1 的汇聚端口信息。

Switch# show port-group 1 port-channel
Port channels in the group 1:

Port-Channel: port-channel1
Number of port : 2   Standby port : NULL

Port in the port-channel :

Index   Port   Mode
----
1   Ethernet0/0/1   active
2   Ethernet0/0/2   active

显示内容	解释
Port channels in the group	如果不存在 port-channel，则不会显示以上打印信息。
Number of port	Port-channel 中的端口数
Standby port	处于 standby 状态的端口，standby 的端口表示虽然端口满足进入 channel 的条件，但由于总共进入 channel 的端口数已经大于最大数，所以将该端口的状态设为 standby 而不是 selected。

15.4.1.2 debug lacp

命令：debug lacp

no debug lacp

功能：打开交换机的 lacp 的调试开关；本命令的 no 操作为关闭该调试开关。

命令模式：特权用户配置模式

缺省情况：缺省关闭交换机的 lacp 的调试开关。

使用指南：用来打开交换机 lacp 调试开关，可以显示交换机处理 lacp 数据包信息。

举例：打开 lacp 调试开关。

Switch#debug lacp

15.4.2 Port Channel 排错帮助

当配置端口聚合功能出现问题时，请检查是否是如下原因：

- 端口聚合组中的端口不具有相同的属性，即双工模式是否为全双工模式，速率是否强制成相同的速率，以及VLAN的属性等。如果检查不相同，则修改成相同；
- 一些命令不能在port-channel上的端口使用，包括：arp，bandwidth，ip，ip-forward等；
- 在使用强制生成端口聚合组时，由于汇聚是手工配置触发的，如果由于端口的VLAN信息不一致导致汇聚失败的话，汇聚组一直会停留在没有汇聚的状态，必须通过往该

group增加和删除端口来触发端口再次汇
聚，如果VLAN信息还是不一致仍然不能汇聚成功。直到VLAN信息都一致并且有增加和删除端口触发汇聚的情况下端口才能汇聚成功；

- 检查对端交换机的对应端口是否配置端口聚合组，且要查看配置方式是否相同，如果本端是手工方式则对端也应该配置成手工方式，如果本端是LACP动态生成则对端也应该是LACP动态生成，否则端口聚合组不能正常工作；还有一点要注意的是如果两端收发的都是LACP协议，至少有一端是ACTIVE的，否则两端都不会发起LACP数据报；
- port-channel一旦形成之后，所有对于端口的设置只能在port-channel端口上进行。

第16章DH
CP 配置

16.1 DHCP 简介

DHCP**[RFC2131]**是 Dynimic Host Configuration Protocol 动态主机配置协议的简写，它能从地址池中把 IP 地址动态分配给请求的主机，同时也能够提供其它网络配置参数，如缺省网关、DNS 服务器、缺省路由和网络范围内主机映像文件的位置等。DHCP 是 BootP 协议功能的增强，与 BootP 相比，DHCP 是主流技术，它不仅能为无盘工作站提供引导信息，而且在大型的网络中可以大大减轻网络管理员跟踪记录手工分配 IP 地址的负担，同时也能减轻用户的配置任务和花费。DHCP 的另外一个优点是可以部分缓解 IP 地址紧张的状况，当某一 IP 地址的用户离开使用环境时，该 IP 地址还能再次分配给其他用户使用。

DHCP 是基于 Client－Server 模式的协议，DHCP 客户机向 DHCP 服务器索取网络地址及配置参数；服务器为客户机提供网络地址及配置参数；当 DHCP 客户机和 DHCP 服务器不在同一子网时，需要由 DHCP 中继为 DHCP 客户机和 DHCP 服务器传递 DHCP 报文。协议实现的过程如下：

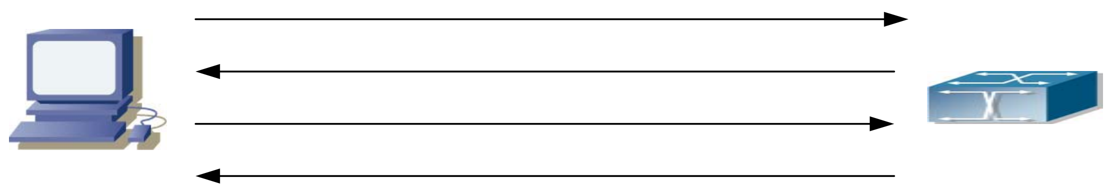


图 16-1 DHCP 协议交互过程

图解：

1. 首先 DHCP 客户机在本子网内广播 DHCPDISCOVER 包；
2. DHCP 服务器收到 DHCPDISCOVER 包后，给该 DHCP 客户机发送带有 IP 地址和其他网络参数的 DHCPOFFER 包；
3. DHCP 客户机对收到的 DHCPOFFER 包进行选择后，广播带有它要选择的 DHCP 服务器的信息的 DHCPREQUSET 包；
4. 被 DHCP 客户机选中的 DHCP 服务器向 DHCP 客户机发送 DHCPACK 包，DHCP 客户机得到 IP 地址和其他网络配置参数。

通过上面四个步骤，完成动态分配主机配置的协议过程。但如果 DHCP 服务器和 DHCP 客户机不在同一网络时，服务器是无法收到客户机发出的 DHCP 广播报文，因此服务器也不会给客户机发送的任何 DHCP 报文，这时需要 DHCP 中继来转发这些 DHCP 报文，完成 DHCP 客户机和服务器之间的 DHCP 报文交互过程。

神州数码交换机实现了 DHCP 服务器和 DHCP 中继的功能。DHCP 服务器不但支持动态分配 IP 地址，还支持手工绑定 IP 地址（即为指定的硬件地址或者指定设备标识的网络设备分配一个固定的长期的 IP 地址）。动态分配 IP 地址和手工绑定 IP 地址的区别和联系是：1)采用动态方式获得的 IP 地址可以是不固定的；而采用手工绑定方式获得的 IP 地址是固定

的；2)采用动态方式获得的 IP 地址租期与其
地址池的租期一致，是有时间限制的；而采用手工绑定方式获得的 IP 地址的租期理论上是无限长时间，即没有时间限制；3)手工绑定 IP 地址的优先级高于动态分配 IP 地址；4)手工 DHCP 地址池可以继承相关网段的动态 DHCP 地址池的网络配置参数。

16.2 DHCP 服务器配置

16.2.1 DHCP 服务器配置任务序列

2. 启动/关闭 DHCP 服务器功能
3. 配置 DHCP 地址池
   （1） 创建/删除 DHCP 地址池
   （2） 配置动态 DHCP 地址池的参数
   （3） 配置手工 DHCP 地址池的参数
4. 启动记录地址冲突的日志功能
5. 配置发 ping 包的个数和超时时间

1.启动/关闭 DHCP 服务

命令	解释
全局配置模式	
service dhcp **no service dhcp**	启动 DHCP 服务器功能。

2.配置 DHCP 地址池

（1）创建/删除 DHCP 地址池

命令	解释
全局配置模式	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	配置 DHCP 地址池。

（2）配置动态 DHCP 地址池的参数

命令	解释
DHCP 地址池配置模式	
network-address <*network-number*> [mask | prefix-length] **no network-address**	配置地址池可分配的地址范围。
default-router [address1[address2[…address8]]] **no default-router**	为 DHCP 客户机配置缺省网关。
dns-server [address1[address2[…address8]]] **no dns-server**	为 DHCP 客户机配置 DNS 服务器。

domain-name <*domain*> **no domain-name**	为 DHCP 客户机配置域名；本命令的 no 操作为删除域名。
netbios-name-server [address1[address2[…address8]]] **no netbios-name-server**	配置 Wins 服务器的地址。
netbios-node-type ｛b-node|h-node|m-node|p-node|<*type-number*>｝ **no netbios-node-type**	配置 DHCP 客户机的节点类型。
bootfile <*filename*> **no bootfile**	配置 DHCP 客户机的启动时的导入文件名。
next-server [address1[address2[…address8]]] **no next-server [address1[address2[…address8]]]**	配置客户机导入文件存放的服务器地址。
option <*code*> {ascii <*string*> | hex <*hex*> | ip <*ipaddress*>} **no option <*code*>**	配置 option 所指定代码的网络参数的值。
lease { days [hours][minutes] | infinite } **no lease**	配置地址池中地址的租用期限。
全局配置模式	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	排除地址池中的不用于动态分配的地址。

（3）配置手工 DHCP 地址池的参数

命令	解释
DHCP 地址池配置模式	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	在手工分配地址时，指定用户的硬件地址。
host <*address*> [<*mask*> | <*prefix-length*>] **no host**	在手工绑定地址时，配置分配给指定客户机的用户的 IP 地址。
client-identifier <*unique-identifier*> **no client-identifier**	在手工绑定地址时，指定用户的唯一标识。
client-name <*name*> **no client-name**	在手工绑定地址时，配置用户名。

3.启动记录地址冲突的日志功能

命令	解释
全局配置模式	

ip dhcp conflict logging **no ip dhcp conflict logging**	打开 DHCP 服务器检测地址冲突的日志功能。
特权用户配置模式	
clear ip dhcp conflict <*address* | *all*>	删除单条地址冲突的记录或全部地址的冲突记录

4.配置发 **ping** 包的个数和超时时间

命令	解释
全局配置模式	
ip dhcp ping packets <*count*> **no ip dhcp ping packets**	配置对地址池中将要被分配的地址的发 ping 的个数。
ip dhcp ping timeout <*milliseconds*> **no ip dhcp ping timeout**	配置发 ping 包后等待收到回应的超时时间。

16.2.2 DHCP 服务器配置命令

16.2.2.1 bootfile

命令：**bootfile <*filename*>**
no bootfile
功能：配置 DHCP 客户机的启动时的导入文件名；本命令的 no 操作为删除该项配置。
参数：**<*filename*>**为导入文件的名字，最长不超过 255 个字节。
命令模式：DHCP 地址池模式
使用指南：为客户机指定导入文件名。一般用在无盘工作站，系统启动时需要从服务器上下载配置文件，和 **next-server** 结合使用。
举例：导入文件地址及文件名为 c:\temp\nos.img
Switch(dhcp-1-config)#bootfile c:\temp\nos.img
相关命令：**next-server**

16.2.2.2 client-identifier

命令：**client-identifier <*unique-identifier*>**
no client-identifier
功能：在手工绑定地址时，指定用户的唯一标识；本命令的 no 操作为删除用户标识。
参数：**<*unique-identifier*>**为用户的标识，格式为点分十六进值。
命令模式：DHCP 地址池模式
使用指南：本命令在手工绑定地址时结合命令 **host** 一起使用。当发出请求的客户机的标识恰好和指定的标识相吻合，DHCP 服务器就将 **host** 命令中定义的 IP 地址分配给客户机。
举例：手工绑定时，将 IP 地址 10.1.128.160 与用户唯一标识为 00-10-5a-60-af-12 的用户绑定。
Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24
相关命令：**host**

16.2.2.3 client-name

命令：**client-name <*name*>**
no client-name
功能：在手工绑定地址时，配置用户名；本命令的 no 操作为删除用户名。
参数：***<name>***为用户的名称，最长不超过 255 字符。
命令模式：DHCP 地址池模式
使用指南：给手工绑定的设备配置用户名，在配置用户名时不应包括域名。
举例：用户唯一标识为 00-10-5a-60-af-12 的用户设置用户名为 network。
Switch(dhcp-1-config)#client-name network

16.2.2.4 default-router

命令：**default-router <*address1*>[<*address2*>[…<*address8*>]]**
no default-router
功能：为 DHCP 客户机配置缺省网关；本命令的 no 操作为删除缺省网关。
参数：***address1…address8*** 为 IP 地址，均为点分十进制格式。
缺省情况：系统没有给 DHCP 客户机配置缺省网关。
命令模式：DHCP 地址池模式
使用指南：缺省网关的 IP 地址应与 DHCP 客户机的 IP 地址在一个子网网段内，交换机最多可支持 8 个网关地址，最先设置的网关地址优先级最高，因此 address1 优先级最高，依次 address2、address3……。
举例：设置 DHCP 客户机的缺省网关为 10.1.128.2 和 10.1.128.100。
Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

16.2.2.5 dns-server

命令：**dns-server <*address1*>[<*address2*>[…<*address8*>]]**
no dns-server
功能：为 DHCP 客户机配置 DNS 服务器；本命令的 no 操作为删除 DNS 服务器。
参数：***address1…address8*** 为 IP 地址，均为点分十进制格式。
缺省情况：系统没有给 DHCP 客户机配置 DNS 服务器。
命令模式：DHCP 地址池模式
使用指南：系统最多可支持配置 8 个 DNS 服务器地址，最先设置的 DNS 服务器的地址优先级最高，因此 address1 优先级最高，依次 address2、address3……。
举例：设置 DHCP 客户机的 DNS 服务器的地址为 10.1.128.3。
Switch(dhcp-1-config)#dns-server 10.1.128.3

16.2.2.6 domain-name

命令：**domain-name <*domain*>**

no domain-name

功能：为 DHCP 客户机配置域名；本命令的 no 操作为删除域名。

参数：*<domain>*为域的名称，最长不超过 255 字符。

命令模式：DHCP 地址池模式

使用指南：为客户机指定域名。

举例：指定 DHCP 客户机的域名为 digitalchina.com.cn

Switch(dhcp-1-config)#domain-name digitalchina.com.cn

16.2.2.7 hardware-address

命令：hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}]

no hardware-address

功能： 在手工分配地址时，指定用户的硬件地址；本命令的 no 操作为删除该项配置。

参数：*<hardware-address>*为硬件地址，十六进值表示的数值；**Ethernet | IEEE802** 为以太网协议类型，***<type-number>***为 RFC 定义的协议类型的数字表示，取值范围为 1~255，如参数 **Ethernet** 的数字表示为 0，**IEEE802** 的数字表示形式为 6。

缺省情况：缺省为协议类型为 Ethernet 协议。

命令模式：DHCP 地址池模式

使用指南：本命令在手工绑定地址时结合命令 **host** 一起使用。当发出请求的客户机的硬件地址恰好和指定的硬件地址相吻合，DHCP 服务器就将 **host** 命令中定义的 IP 地址分配给客户机。

举例：手工绑定时，将 IP 地址 10.1.128.160 与硬件地址为 00-00-e2-3a-26-04 的用户绑定。

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

相关命令：host

16.2.2.8 host

命令：host <*address*> [<*mask*> | <*prefix-length*>]

no host

功能：在手工绑定地址时，分配给指定客户机的用户的 IP 地址；本命令的 no 操作为删除 IP 地址。

参数：*<address>*为 IP 地址，点分十进制格式；***<mask>***为掩码，点分十进制格式；***<prefix-length>***为用前缀表示法，如掩码为 255.255.255.0 用前缀法表示为"24"，掩码为 255.255.255.252 用前缀法表示为"30"。

命令模式：DHCP 地址池模式

使用指南：如果在配置 IP 地址时，仅配置了 IP 地址，没有配置掩码和前缀，并且在 IP 地址池中也没有任何有关掩码的信息，缺省系统会按有类地址自动分配掩码。

本命令在手工绑定地址时结合 **hardware-address** 命令或者 **client-identifier** 命令一起使用。当发出请求的客户机的标识或硬件地址恰好和指定的标识或硬件地址相吻合，DHCP 服务器就将 **host** 命令中定义的 IP 地址分配给客户机。

举例：手工绑定时，将 IP 地址 10.1.128.160 与硬件地址为 00-10-5a-60-af-12 的用户绑定。

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

相 关 命 令 ： **hardware-address** 、 **client-identifier**

16.2.2.9 ip dhcp conflict logging

命令：ip dhcp conflict logging
no ip dhcp conflict logging
功能：打开 DHCP 服务器检测地址冲突的日志功能；本命令的 no 操作为关闭该日志功能。
缺省情况：缺省情况下，记录地址冲突的日志功能是打开的。
命令模式：全局配置模式
使用指南：当日志功能是打开的，一旦 DHCP 服务器检测到有地址冲突时，就会将该冲突地址记录到日志中。对于在日志中出现的有冲突记录的地址，DHCP 服务器将不再对其进行动态分配，直到把这些冲突记录删除。
举例：关闭 DHCP 服务器的日志功能。
Switch(Config)#no ip dhcp conflict logging
相关命令：clear ip dhcp conflict

16.2.2.10 ip dhcp excluded-address

命令：ip dhcp excluded-address <*low-address*> [<*high-address*>]
no ip dhcp excluded-address <*low-address*> [<*high-address*>]
功能：排除地址池中的不用于动态分配的地址；本命令的 no 操作为取消该项配置。
参数：<*low-address*>为起始的 IP 地址；**[<*high-address*>]**为结束的 IP 地址。
缺省情况：缺省为仅排除单个地址。
命令模式：全局配置模式
使用指南：使用本命令可以将地址池中的一个地址或连续的几个地址排除，这些地址由系统管理员留作其它用途。
举例：将 10.1.128.1 到 10.1.128.10 之间的地址保留，不用于动态分配。
Switch(Config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

16.2.2.11 ip dhcp pool

命令：ip dhcp pool <*name*>
no ip dhcp pool <*name*>
功能：配置 DHCP 地址池，进入 dhcp 地址池模式；本命令的 no 操作为删除该地址池。
参数：<*name*>为地址池名，最长不超过 255 个字符。
命令模式：全局配置模式
使用指南：在全局模式下定义一个 DHCP 地址池，进入到 DHCP 地址池配置模式。
举例：定义一个地址池，取名 1。
Switch(Config)#ip dhcp pool 1
Switch(dhcp-1-config)#

16.2.2.12 ip dhcp ping packets

命令：ip dhcp ping packets <*count*>

no ip dhcp ping packets

功能：配置对地址池中即将要分配的地址的发 ping 包的个数；本命令的 no 操作为恢复缺省值。

参数：<*count*>发包个数，取值范围 0~10。

缺省情况：缺省为 2 个。

命令模式：全局配置模式

使用指南：配置发 ping 的个数，系统缺省为 2 个。

举例：修改发 ping 包的个数为 5 个。

Switch(Config)#ip dhcp ping packets 5

相关命令：ip dhcp ping timeout

16.2.2.13 ip dhcp ping timeout

命令：ip dhcp ping timeout <*milliseconds*>

no ip dhcp ping timeout

功能：配置发 ping 包后等待收到回应的超时时间；本命令的 no 操作为恢复缺省值。

参数：<*milliseconds*>为超时时间值，单位为毫秒，取值范围为 100~10000。

缺省情况：缺省为 500 毫秒。

命令模式：全局配置模式

使用指南：配置接收 ping 包回应的超时时间，在指定时间内 DHCP 服务器没有接收 ping 的回应，DHCP 服务器就认为该地址未被使用，就将该 IP 地址分配给客户机；如果收到回应，则记录该地址到冲突日志中。

举例：修改超时时间为 1 秒钟。

Switch(Config)#ip dhcp ping timeout 1000

相关命令：ip dhcp ping packets

16.2.2.14 loghost dhcp

命令：loghost dhcp <*ip-address*> <*port*>

no loghost dhcp

功能：打开 DHCP 的日志功能，并且指定 DHCP 日志主机的 IP 地址及端口号；本命令的 no 操作为关闭 DHCP 日志功能。

参数：<*ip-address*>为记录 DHCP 日志的主机 IP 地址，点分十进制格式；**<*port*>**为端口号，取值范围为 0~65535。

缺省情况：缺省不打开 DHCP 日志功能。

命令模式：全局配置模式

使用指南：用户在配置了本命令后可到相应的日志主机上查看有关 DHCP 地址分配的各项记录。执行神州数码网络（北京）有限公司提供的 logtest.exe 程序的主机就可以成为 DHCP 日志主机。

举例：打开 DHCP 日志功能，日志主机为 192.168.1.101，端口号为 45。

Switch(Config)#loghost dhcp 192.168.1.101 45

16.2.2.15 lease

命 令 ： **lease { [<*days*>] [<*hours*>][<*minutes*>] | infinite }**

no lease

功能：配置地址池中地址的租用期限；本命令的 no 操作为恢复缺省值。

参数：<*days*>为天数，取值范围为 0~365；**<*hours*>**为小时数，取值范围为 0~23；**<*minutes*>**为分数，取值范围为 0~59；**infinite** 为永久的使用。

缺省情况：缺省的租期设置为 1 天。

命令模式：DHCP 地址池模式

使用指南：DHCP 是动态的分配网络配置参数，并非永久分配，因此有租期的限制。租期设置过长，难以发挥 DHCP 灵活、动态的优势；租期设置过短，有会造成网络通信量的增加，加大网络开销，因此租期的设置可由网络管理员根据自身网络的特点设定。

举例：DHCP 地址池 1 的租期设置为 3 天 12 个小时 30 分钟。

Switch(dhcp-1-config)#lease 3 12 30

16.2.2.16 netbios-name-server

命令：netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]

no netbios-name-server

功能：配置 Wins 服务器的地址；本命令的 no 操作为删除 Wins 服务器。

参数：*address1…address8* 为 IP 地址，均为点分十进制格式。

缺省情况：系统缺省没有配置 Wins 服务器。

命令模式：DHCP 地址池模式

使用指南：为客户机指定 WINS 服务器，最多可设置 8 个 WINS 服务器，最先设置的 Wins 服务器的地址优先级最高，因此 address1 优先级最高，依次 address2、address3……。

16.2.2.17 netbios-node-type

命令：netbios-node-type ｛**b-node|h-node|m-node|p-node|<*type-number*>**｝

no netbios-node-type

功能：配置 DHCP 客户机的节点类型；本命令的 no 操作为取消该项配置。

参数：b-node 为广播型；**h-node** 为先点对点后广播的混合型；**m-node** 为先广播后点对点的混合型；**p-node** 为点对点型；**<*type-number*>**为节点类型的十六进值表示法，取值范围为 0~FF。

缺省情况：没有为客户机指定节点类型。

命令模式：DHCP 地址池模式

使用指南：如果要为客户机指定节点类型，建议把客户机的节点类型配置为先点对点后广播的混合型节点类型。

举例：地址池 1 的客户机的节点类型为广播型。

Switch(dhcp-1-config)#netbios-node-type b-node

16.2.2.18 network-address

命令：network-address <*network-number*> [<*mask*> | <*prefix-length*>]

no network-address

功能：配置地址池可分配的地址范围；本命令
的 no 操作为取消该项配置。

参数：***<network-number>***为网络号码；***<mask>***为掩码，点分十进制格式；***<prefix-length>***为用前缀表示法，如掩码为 255.255.255.0 用前缀法表示为“24”，掩码为 255.255.255.252 用前缀法表示为“30”。

缺省情况：如果不带掩码，缺省掩码为按照有类地址自动分配。

命令模式：DHCP 地址池模式

使用指南：DHCP 服务器用于动态分配 IP 地址时使用本命令配置可分配的 IP 地址范围，一个地址池只能对应一个网段。本命令与手工绑定地址的命令即 **hardware-address** 命令、**host** 命令互斥。

举例：地址池 1 的可分配的地址为 10.1.128.0/24。

Switch(dhcp-1-config)#network-address 10.1.128.0 24

相关命令：ip dhcp excluded-address

16.2.2.19 next-server

命令：next-server <*address1*>[<*address2*>[…<*address8*>]]

no next-server

功能：配置客户机导入文件存放的服务器地址；本命令的 no 操作为取消该项配置。

参数：***address1…address8*** 为 IP 地址，均为点分十进制格式。

命令模式：DHCP 地址池模式

使用指南：为客户机指定导入文件存放的服务器地址。一般用在无盘工作站，系统启动时需要从服务器上下载配置文件，和 **bootfile** 结合使用。

举例：文件存放的服务器地址为 10.1.128.4。

Switch(dhcp-config)#next-server 10.1.128.4

相关命令：bootfile

16.2.2.20 option

命令：option <*code*> {ascii <*string*> | hex <*hex*> | ip <*ipaddress*>}

no option <*code*>

功能：配置 option 所指定代码的网络参数的值；本命令的 no 操作为取消对该 option 的配置。

参数：***<code>***为网络参数的代码值；***<string>***为 ASCⅡ型字符串，最长不超过 255 个字符；***<hex>***为十六进值表示的数值，最长不超过 510，且长度必须为偶数；***<ipaddress>***为 IP 地址，点分十进制格式，最长可以设置 63 个 IP 地址。

命令模式：DHCP 地址池模式

使用指南：系统不仅提供多项在网络配置中常用的命令，还提供了配置网络参数的通用命令，满足用户的多方面的配置需求。Option 的代码定义在 **RFC2132** 中有详细介绍。

举例：配置 WWW 服务器的地址为 10.1.128.240。

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

16.2.2.21 service dhcp

命令：service dhcp

no service dhcp

功能：启动 DHCP 服务器功能；本命令的 no 操作为关闭 DHCP 服务。

缺省情况：DHCP 服务缺省是关闭的。

命令模式：全局配置模式

使用指南：DHCP 服务包括 DHCP 服务器功能和 DHCP 中继的功能。当打开 DHCP 服务时，DHCP 服务器功能和 DHCP 中继功能都被打开。只有打开 DHCP 服务器功能，才能给 DHCP 客户机分配 IP 地址及其它网络参数。

举例：打开 DHCP 服务器。

Switch(Config)#service dhcp

16.3 DHCP 中继配置

当 DHCP 客户机和 DHCP 服务器不在同一个网段时，由 DHCP 中继传递 DHCP 报文。增加 DHCP 中继功能的好处是不必为每个网段都设置 DHCP 服务器，同一个 DHCP 服务器可以为很多个子网的客户机提供网络配置参数，即节约了成本又方便了管理。

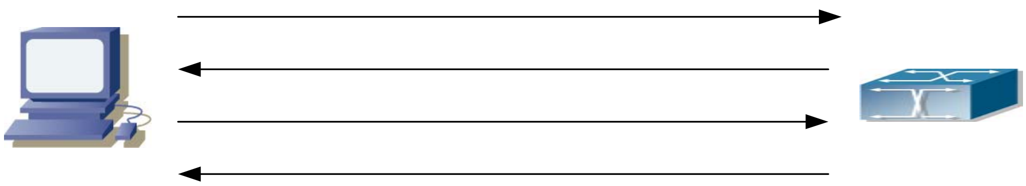


图 16-2 DHCP 中继

如上图所示，DHCP 客户机和 DHCP 服务器不在一个网络内，DHCP 客户机仍然遵循 DHCP 的四个步骤，但增加了 DHCP 中继的转发功能：

1. 首先广播 DHCPDISCOVER 报文，DHCP 中继接收到客户机广播的 DHCPDISCOVER 文后，在该报文的中继代理字段处加入自己的 IP 地址后转发给指定的 DHCP 服务器（有关 DHCP 帧格式可参看 RFC2131）；
2. DHCP 服务器接收到经过 DHCP 中继转发的 DHCPDISCOVER 后，带有网络配置参数的 DHCPOFFER 报文经过 DHCP 中继发送给 DHCP 客户机；
3. DHCP 客户机选中一个 DHCP 服务器，广播 DHCPREPLY 报文，DHCP 中继的处理该报文后转发给 DHCP 服务器；
4. DHCP 服务器收到 DHCPREPLY 后，回应 DHCPACK 报文经过 DHCP 中继发送给 DHCP 客户机。

DHCP 中继除了能将 DHCP 的广播报文转发到指定的 DHCP 服务器，还能转发其他特定协议的 UDP 广播报文转发到指定的服务器中。

16.3.1 DHCP 中继配置任务序列

1. 启动 DHCP 中继
2. 配置 DHCP 中继转发 DHCP 广播报文
3. 配置 DHCP 中继转发其他 UDP 广播报文
4. 禁止 DHCP 中继转发 DHCP 广播报文

1.启动 DHCP 中继

在前面 15.2.1 中曾讲到启动 DHCP 服务时即启动了 DHCP 服务器的功能，又启动了 DHCP 中继的功能。（详见 15.1.2.1 相关内容）

2.配置 DHCP 中继转发 DHCP 广播报文

命令	解释
接口配置模式	
ip forward-protocol udp <*port*> **no ip forward-protocol udp <*port*>**	转发 DHCP 广播报文时，UDP 端口号为 67。
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	指定 DHCP 中继转发的目标 IP 地址；本命令的 no 操作为取消该项配置。

3.配置 DHCP 中继转发其他 UDP 广播报文

命令	解释
全局配置模式	
ip forward-protocol udp <*port*> **no ip forward-protocol udp <*port*>**	通过配置 UDP 端口，指定 DHCP 中继转发协议；本命令的 no 操作为取消该项配置。
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	指定 DHCP 中继转发的目标 IP 地址；本命令的 no 操作为取消该项配置。

4. 禁止 DHCP 中继转发 DHCP 广播报文

命令	解释
全局配置模式	
ip dhcp relay information policy drop **no ip dhcp relay information policy drop**	三层交换机作为 DHCP 中继时，配置中继的转发政策为不转发 DHCP 报文；本命令的 no 操作为恢复转发 DHCP 报文。

16.3.2 DHCP 中继配置命令

16.3.2.1 ip forward-protocol udp

命令：ip forward-protocol udp <port>

no ip forward-protocol udp <port>

功能：配置 DHCP 中继转发 port 端口的 udp 广播报文；本命令的的 no 操作为取消该项服务。

缺省情况：DHCP 中继缺省转发 DHCP 广播报文（udp 端口为 67）。

命令模式：全局配置模式

使用指南：该命令的转发目的地址在随后的 ip helper-address 命令里设定

举例：转发 tftp 包，且目的服务器地址为 192.168.1.5。

Switch(Config)#ip forward-protocol udp 69
Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip helper-address
192.168.1.5

16.3.2.2 ip helper-address

命令：ip helper-address <*ip-address*>

no ip helper-address <*ip-address*>

功能：指定 DHCP 中继转发 udp 报文的目标地址。；本命令的的 no 操作为取消该项设置。

缺省情况：DHCP 中继缺省设置成转发 DHCP 广播报文的地址。

命令模式：接口配置模式

使用指南：DHCP 中继转发的服务器地址是与转发 UDP 的端口相对应的，即 DHCP 中继只转发相应 UDP 协议的报文给相应的服务器，并不是把所有 UDP 报文转发给所有的服务器，缺省配置时 DHCP 中继转发的是 UDP 端口为 67 的 DHCP 报文给 DHCP 服务器。当使用 **ip forward-protocol udp <*port*>**命令后，再配置本命令时，本命令所配置的转发地址接收到的是端口号为**<*port*>**的 UDP 报文，而非缺省时的 DHCP 报文。如果要配置另外一组 UDP 转发协议及接收服务器地址，则需另外使用命令 **ip forward-protocol udp <*port*>**和本命令的组合进行配置。更详细的配置情况参看 DHCP 配置案例的相关部分。

举例：

16.3.2.3 ip dhcp relay information policy drop

命令：ip dhcp relay information policy drop

no ip dhcp relay information policy drop

功能：三层交换机作为 DHCP 中继时，配置中继的转发政策为不转发 DHCP 报文；本命令的 no 操作为恢复转发 DHCP 报文。

缺省情况：DHCP 中继缺省转发 DHCP 广播报文

命令模式：全局配置模式

使用指南：当 DHCP 中继因为特殊原因不应该转发 DHCP 报文时，可以使用本命令关闭 DHCP 中继转发 DHCP 报文的功能。

举例：关闭三层交换机 DHCP 广播报文转发功能。

Switch(Config)# ip dhcp relay information policy drop

16.4 DHCP 配置举例

案例 1：

为减轻网络管理员和用户的配置负担，现有某公司将神州数码交换机作为 DHCP 服务器。其 Admin VLAN 的 IP 地址为 10.16.1.2/24。其中公司局域网因为办公地点分成了 A 地、B 地两部分，A 地、B 地的网络配置如下表。

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
设备	Ip 地址	设备	Ip 地址
缺省网关	10.16.1.200	缺省网关	10.16.2.200

	10.16.1.201		10.16.2.201
DNS 服务器	10.16.1.202	DNS 服务器	10.16.2.202
Wins 服务器	10.16.1.209	WWW 服务器	10.16.2.209
Wins 的节点类型	H-node		
Lease	3 天	Lease	1 天

其中在 A 处，因为工作的需要，特地将一台 MAC 地址为 00-03-22-23-dc-ab 的机器分配固定的 IP 地址 10.16.1.210，命名为 management。

Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.16.1.2 255.255.255.0
Switch(Config-If-Vlan1)#exit
Switch(Config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(Config)#ip dhcp excluded-address 10.16.1.200 10.16.1.210
Switch(Config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(Config)#ip dhcp excluded-address 10.16.2.200 10.16.2.210
Switch(Config)#ip dhcp pool A1
Switch(dhcp-A1config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 0003.2223.dcab
Switch(dhcp-A1-config)#client-name management
Switch(dhcp-A1-config)#exit

案例 2：

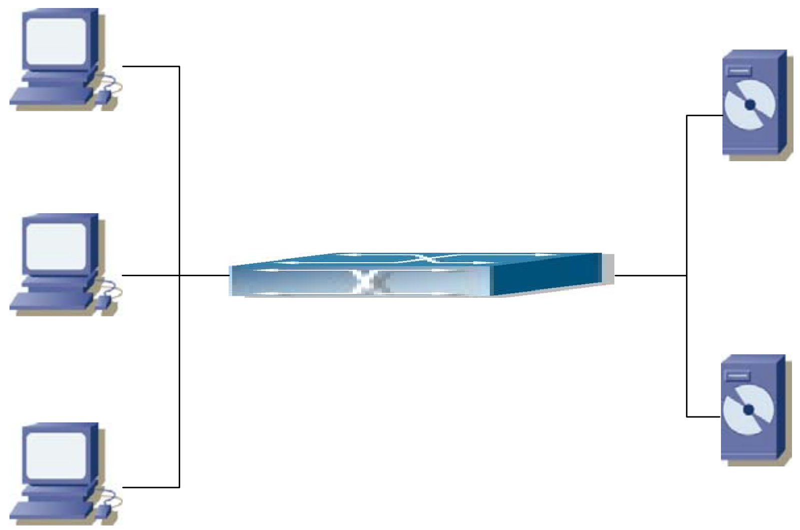


图 16-3 DHCP Relay 配置

如图所示，配置 DCRS 为 DHCP 中继。DHCP 服务器的地址为 10.1.1.10，TFTP 服务器的地址为 10.1.1.20，则配置如下：

```
switch(Config)#interface vlan 1
switch (Config-If-Vlan1)#ip address 192.168.1.1 255.255.255.0
switch (Config-If-Vlan1)#exit
switch(Config)#interface vlan 2
switch (Config-If-Vlan2)#ip address 10.1.1.1 255.255.255.0
switch (Config-If-Vlan2)#exit
switch(Config)#ip forward-protocol udp 67
switch(Config)#interface vlan 1
switch (Config-If-Vlan1)#ip help-address 10.1.1.10
switch (Config-If-Vlan1)#exit
switch (Config)#ip forward-protocol udp 69
switch (Config)#interface vlan 1
switch (Config-If-Vlan1)#ip help-address 10.1.1.20
```

注意：DHCP 服务器地址和 TFTP 服务器地址必须分开配置，因为它们所接收的 UDP 协议是不同的。建议配置命令 **ip forward-protocol udp** ***<port>*** 和 **ip helper-address** ***<ipaddress>***结合使用。**ip help-address** 只能在三层端口下配置，不能直接在二层端口下配置。

使用提示：

当有 DHCP/BootP Client 连接在交换机的属于 VLAN1 端口时，该 Client 只能获取属于 10.16.1.0/24 网段的地址而不可能获取 10.16.2.0/24 网段的地址。因为 Client 发出的广播包经过交换机的 VLAN 接口转发后，申请的是与 VLAN 接口在一个网段的 IP 地址，交换机的 VLAN 接口的 IP 地址为 10.16.1.2/24，因此 Client 申请到的 IP 地址是 10.16.1.0/24 网段的。若 DHCP/BootP Client 希望申请到 10.16.2.0/24 网段的地址，该 Client 发出的广播包经由

转发的网关必须是 10.16.2.0/24 网段的。若要
从交换机获取 10.16.2.0/24 地址池的 IP 地址，则首先要保证该 Client 的网关到交换机的可达性。

16.5 DHCP 排错帮助

16.5.1 监测和调试的命令

16.5.1.1 clear ip dhcp binding

命令：clear ip dhcp binding {<*address*> | all }
功能：删除某指定的 IP 地址与其硬件地址的绑定记录或所有 IP 地址与相应的硬件地址的绑定记录。
参数：<*address*>为指定的有绑定记录的 IP 地址，点分十进制格式；**all** 通指为有绑定记录的所有的 IP 地址。
命令模式：特权用户配置模式
使用指南：通过 **show ip dhcp binding** 命令可以查看 IP 地址与相应的 DHCP 客户机硬件地址的绑定信息，当 DHCP 服务器得知某 DHCP 客户机因为特殊原因没有使用分配的 IP 地址但规定的租期未到，DHCP 服务器不会自动解除该绑定信息，此时系统管理员可以使用本命令手工删除该 IP 地址与客户机硬件地址的自动绑定；如果使用 **all**，将删除所有自动绑定记录，这样 DHCP 地址池中的所有地址将被重新分配。
举例：删除所有 IP 地址与硬件地址的绑定记录。
Switch#clear ip dhcp binding all
相关命令：show ip dhcp binding

16.5.1.2 clear ip dhcp conflict

命令：clear ip dhcp conflict {<*address*> | all }
功能：删除在地址冲突日志中有冲突记录的地址。
参数：<*address*>为某指定的有冲突记录的地址；**all** 通指为有冲突记录的所有地址。
命令模式：特权用户配置模式
使用指南：通过 **show ip dhcp conflict** 命令可以查看哪些 IP 地址在使用上有冲突，使用本命令可以删除某一地址的冲突记录，如果使用 **all** 则是删除日志中所有的地址的冲突记录。在日志中删除冲突记录后，这些地址可被 DHCP 服务器重新使用。
举例：网络管理员查看冲突日志文件，发现文件中有冲突记录的 10.1.128.160 地址现已无人使用，将该地址的记录从地址冲突文件中。
Switch#clear ip dhcp conflict 10.1.128.160
相关命令：ip dhcp conflict logging，show ip dhcp conflict

16.5.1.3 clear ip dhcp server statistics

命令：clear ip dhcp server statistics

功能：删除 DHCP 服务器的统计记录，将
DHCP 服务器的计数器清零。
命令模式：特权用户配置模式
使用指南：通过 **show ip dhcp server statistics** 命令可以查看 DHCP 服务器的计数器的统计信息，所有的统计信息都是一个累计值，使用本命令可以将计数器清零，方便统计信息的查看。
举例：将 DHCP 服务器的计数器清零。
Switch#clear ip dhcp server statistics
相关命令：show ip dhcp server statistics

16.5.1.4 show ip dhcp binding

命令：show ip dhcp binding
功能：显示 IP 地址与 MAC 地址的绑定情况。
命令模式：特权用户配置模式
举例：

```
Switch#sh ip dhcp binding
IP address        Hardware address        Lease expiration     Type
10.1.1.233        00-00-E2-3A-26-04         Infinite             Manual
10.1.1.254        00-00-E2-3A-5C-D3         60                   Automatic
```

显示信息	解释
IP address	分配给 DHCP 客户机的 IP 地址；
Hardware address	DHCP 客户机的硬件地址；
Lease expiration	DHCP 客户机拥有该 IP 地址的有效时间；
Type	类型，指手工绑定还是动态分配的。

16.5.1.5 show ip dhcp conflict

命令：show ip dhcp conflict
功能：显示有冲突记录的地址的日志信息。
命令模式：特权用户配置模式
举例：

```
Switch#sh ip dhcp conflict
IP Address              Detection method        Detection Time
10.1.1.1                Ping                 FRI JAN 02 00:07:01 2002
```

显示信息	解释
IP Address	有冲突的 IP 地址；
Detection method	检测到冲突的方式；
Detection Time	检测到冲突的时间。

16.5.1.6 show ip dhcp server statistics

命令：show ip dhcp server statistics
功能：显示 DHCP 服务器的对各种 DHCP 数据包的统计信息。
命令模式：特权用户配置模式
举例：

```
Switch#sh ip dhcp server statistics
Memory usage                389
Address pools               3
Database agents             0
Automatic bindings          2
Manual bindings             0
Conflict bindings           0
Expiried bindings           0
Malformed message           0

Message                     Recieved
BOOTREQUEST                 3814
DHCPDISCOVER                1899
DHCPREQUEST                 6
DHCPDECLINE                 0
DHCPRELEASE                 1
DHCPINFORM                  1

Message                     Send
BOOTREPLY                   1911
DHCPOFFER                   6
DHCPACK                     6
DHCPNAK                     0
DHCPRELAY                   1907
DHCPFORWARD                 0
Switch#
```

显示信息	解释
Memory usage	内存的利用率；
Address pools	配置的 DHCP 地址池个数；
Database agents	代理数据库的个数；
Automatic bindings	自动分配地址的个数；
Manual bindings	手工绑定地址的个数；
Conflict bindings	有地址冲突的个数；
Expiried bindings	绑定超期的个数；
Malformed message	错误信息的个数；
Message Recieved	接收 DHCP 数据包的统计

BOOTREQUEST	接收的数据包总数；
DHCPDISCOVER	其中 DHCPDISCOVER 包个数；
DHCPREQUEST	其中 DHCPREQUEST 包个数；
DHCPDECLINE	其中 DHCPDECLINE 包个数；
DHCPRELEASE	其中 DHCPRELEASE 包个数；
DHCPINFORM	其中 DHCPINFORM 包个数；
Message Send	发送 DHCP 数据包的统计
BOOTREPLY	发送的数据包的总数；
DHCPOFFER	其中 DHCPOFFER 包的个数；
DHCPACK	其中 DHCPACK 包的个数；
DHCPNAK	其中 DHCPNAK 包的个数；
DHCPRELAY	其中 DHCPRELAY 包的个数；
DHCPFORWARD	其中 DHCPFORWARD 包的个数。

16.5.1.7 debug ip dhcp server

命令：debug ip dhcp server { events|linkage|packets }
no debug ip dhcp server { events|linkage|packets }
功能：打开 DHCP 服务器的调试信息；本命令的 no 操作为关闭 DHCP 服务器的调试信息。
缺省情况：缺省调试开关是关闭的。
命令模式：特权用户配置模式

16.5.2 DHCP 排错帮助

DHCP 客户机无法获得 IP 地址及其它网络参数，在确保 DHCP 客户机硬件、线缆等没有问题的前提下，检查可能存在的情况和建议的解决方法：

- 首先检查 DHCP 服务器是否已启动，若没有启动，建议启动相关的 DHCP 服务器；
- 若 DHCP 客户机和服务器不在同一个物理网络中，检查中间负责转发 DHCP 报文的路由器是否具备 DHCP 中继功能。若中间路由器不具备 DHCP 中继功能，建议替换掉中间的路由器或更新版本，使其具备 DHCP 中继功能；
- 用户比较容易遇到的现象是 DHCP 客户机连接在交换机上，却获得不到 IP 地址。遇到这种情况请检测 DHCP Server 内是否有与交换机 VLAN 接口在一个网段的地址池，如没有则请添加该网段的地址池；（这并不意味 DCS 不具备给其他网段分配 IP 地址的能力，参见第二条解决方法。）
- 在 DHCP 服务中，动态分配 IP 地址与手工分配 IP 地址的地址池是互斥的，即如果在一个地址池执行命令 **network** 和命令 **host** 时，只能有一个生效；并且在手工地址池中一个地址池内只能配置一对 IP-MAC 的绑定，如果需要建立多对绑定，可以建立多个手工地址池，在每个地址池分别配置 IP-MAC 的绑定，否则在同一地址池内配置新的配置会覆盖旧的配置。

第17章SNTP 配置

NTP (the Network Time Protocol)协议广泛用于维持全球 Internet 中的计算机的时钟同步。NTP 协议可以估算封包在网络上的往返延迟外，还可独立地估算计算机时钟偏差，从而实现在网络上的高精准度计算机校时。在大多数地方，根据同步源的特性和网络路径，NTP 提供 1~50ms 的精度。

SNTP（Simple Network Time Protocol）是 NTP 协议的简化版本，除去了 NTP 复杂的算法。SNTP 用于那些不需要完整 NTP 实现复杂性的主机，它是 NTP 的一个子集。通常让局域网上的若干台主机通过因特网与其他的 NTP 主机同步时钟，接着再向局域网内其他客户端提供时间同步服务。下图描画了一个 NTP/SNTP 的应用网络结构，其中 SNTP 主要工作在二级服务器和各种终端之间，主要是由于这些场景时间精度要求不高，而 SNTP 本身可以提供的时间精度（1－50ms）一般可以满足这些服务的应用。

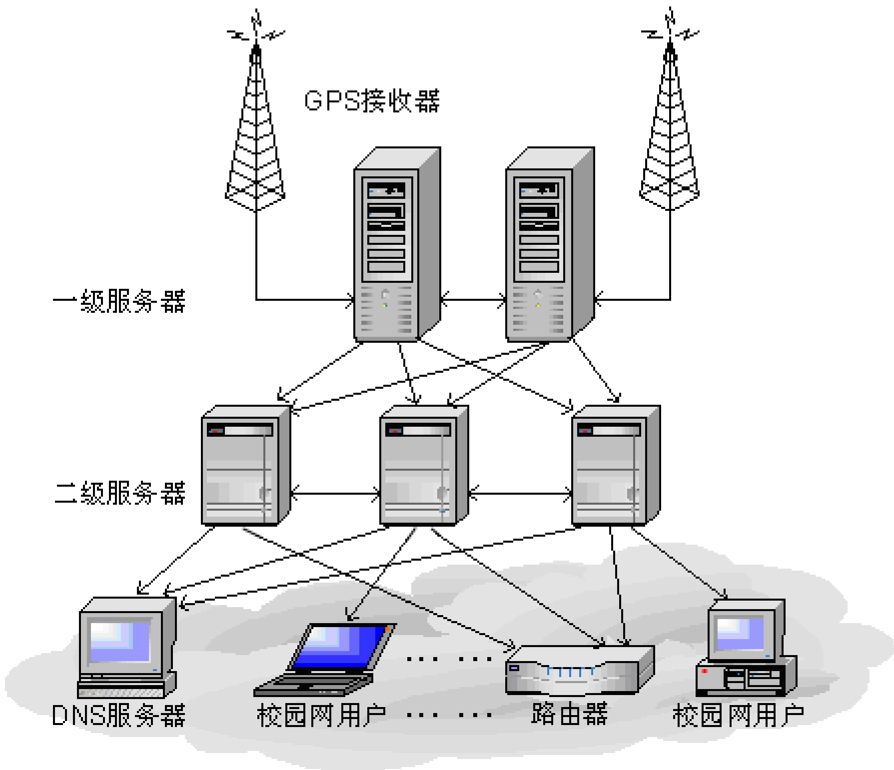


图 17-1 NTP/SNTP 工作场景

神州数码交换机实现了 SNTPv4 的客户端，支持 RFC2030 描述的 SNTP 客户端单播模式（unicast）的协议行为，不支持 SNTP 客户端组播模式（multicast）和任播模式（anycast），也不支持 SNTP 服务器端功能。

17.1 SNTP 配置命令

17.1.1 sntp server

命令：sntp server <*server_address*> [version <*version_no*>]
no sntp server <*server_address*>
功能：设置 SNTP/NTP 服务器地址以及服务器版本；本命令的 no 操作取消设置的 SNTP/NTP 服务器地址。
参数：<*server_address*>为 SNTP/NTP 服务器的 IP 单播地址，**<*version_no*>**为当前客户端的 SNTP 版本号，取值<1-4>。版本默认为 1。
缺省情况：出厂时缺省无该配置
命令模式：全局配置模式
举例：配置一个 SNTP/NTP 服务器地址
Switch(Config)#sntp server 10.1.1.1 version 4

17.1.2 sntp polltime

命令：sntp polltime <*interval*>
no sntp polltime
功能：设置 SNTP 客户端向 NTP/SNTP 服务器发送请求的间隔；本命令的 no 操作取消设置的 polltime，恢复缺省值 64s。
参数：<*interval*> 为要设置的间隔，范围从 16~16284。
缺省情况：polltime 缺省为 64s。
命令模式：全局配置模式
举例：设客户端每隔 128 秒向服务器请求一次。
Switch#config
Switch(Config)#sntp polltime 128

17.1.3 sntp timezone

命令：sntp timezone <*name*> *{add | subtract}* <*time_difference*>
no sntp timezone
功能：设置 SNTP 客户端所在的时区与 UTC 的时差；本命令的 no 操作取消设置的时区，恢复缺省值。
参数：<*name*>为设置的时区名称，不超过 16 个字符，**<*add*>**表示所设时区为 UTC 时间加上**<*time_difference*>**，**<*subtract*>**表示所设时区为 UTC 时间减去**<*time_difference*>**，**<*time_difference*>** 为要设置的时差，范围从 1~12。
缺省情况：缺省时差设为 add 8。
命令模式：全局配置模式
举例：设置时区为 beijing
Switch#config

Switch(Config)#sntp timezone beijing add 8

17.1.4 show sntp

命令：**show sntp**
功能：显示 SNTP 客户端目前的配置及服务器状态。
参数：无
命令模式：特权用户配置模式
举例：显示 SNTP 当前配置
Switch#show sntp
SNTP server Stratum Version Last Receive
2.1.0.2 1 1 never

显示信息	解释
SNTP server	SNTP server 的 IP 地址；
Stratum	SNTP server 所处层数；
Version	SNTP 协议的版本号；
Last Receive	最后接收到 SNTP server 的 IP 地址

17.1.5 debug sntp

命令：**debug sntp {adjust | packet | select }**
no debug sntp {adjust | packet | select}
功能：显示或关闭 SNTP 调试信息。
参数：**adjust** – SNTP 时钟调节信息；**packet** – SNTP 报文；**select** – SNTP 时钟选择。
命令模式：特权用户配置模式
举例：显示 SNTP 协议报文的调试信息
Switch#debug sntp packet

17.2 SNTP 典型配置举例

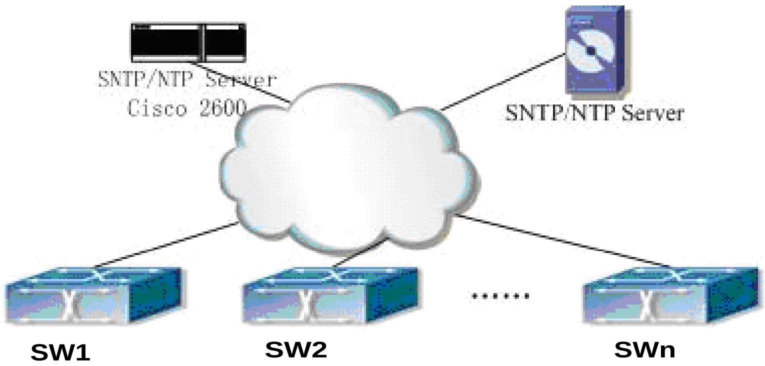


图 17-2 SNTP 典型配置

在自治系统域内的所有神州数码交换机需要进行时间同步，时间同步是通过两台冗余的 SNTP/NTP 服务器实现。为达到时间同步，当前网络必须正确配置，任意一台神州数码交换机和两台 SNTP/NTP 服务器间有可达的路由。设两个 SNTP/NTP Server 的 IP 地址分别配置为 10.1.1.1 和 20.1.1.1，并且已经开启 SNTP/NTP 服务器端功能（如 ntp master）则任意一台神州数码交换机配置如下：

Switch #config

Switch (config)#sntp server 10.1.1.1

Switch (config)#sntp server 20.1.1.1

之后 SNTP 就按照默认的设置（polltime 64s, version 1）与服务器进行时间同步了。

第18章QoS 配置

18.1 QoS 介绍

QoS（Quality of Service，服务品质保证）是指一个网络能够利用各种各样的技术向选定的网络通信提供更好的服务的能力。QoS 是服务品质保证，提供稳定、可预测的数据传送服务，来满足使用程序的要求，QoS 不能产生新的带宽，而是根据应用的需求以及网络管理的设置来有效的管理网络带宽。

18.1.1 QoS 术语

CoS：Class of Service 服务级别，L2 802.1Q 帧携带的分类信息，在帧头的 Tag 字段中占 3bits，称为用户优先级，范围为 0～7。

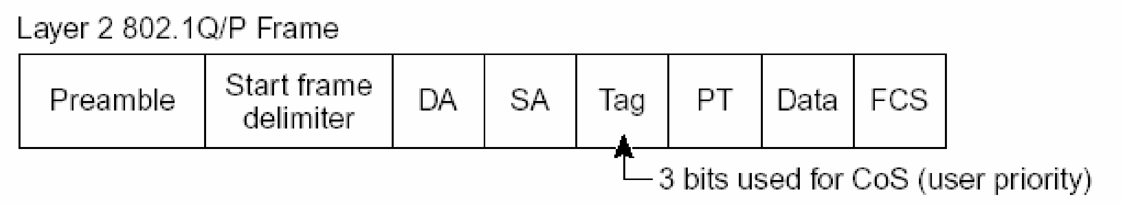


图 1-1 CoS 优先级

ToS：Type of Service 服务类型，L3 IPv4 包头携带的一个字节的字段，标记 IP 包的服务类型，ToS 字段内可以是 IP Precedence 值，也可以是 DSCP 值。

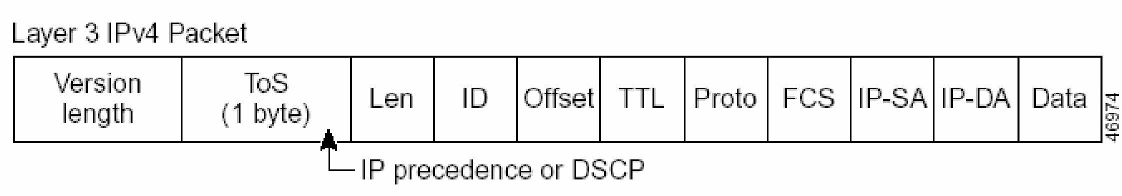


图 1-2ToS 优先级

IP Precedence：IP 优先级，L3 IP 包头携带的分类信息，共占 3bits，范围为 0～7。
DSCP：Differentiated Services Code Point 差别化业务编码点，L3 IP 包头携带的分类信息，共占 6bits，范围为 0～63，向下兼容 IP Precedence。
分类：QoS 的入口动作，根据数据包携带的分类信息和 ACLs，将数据包流量进行分类。
监管：QoS 的入口动作，制定监管策略，对分类后的数据包进行监管。
重写：QoS 的入口动作，根据制定的监管策略，对数据包进行通过、降级、丢包等操作。
整形：QoS 的出口动作，根据数据包的 CoS 值，将其归入相应的出口队列。

排程：QoS 的出口动作，配置四条出口队列的 WRR（Weighted Round Robin）权重。

In Profile：对于在 QoS 监管策略规定范围（带宽或突发值）内的流量，我们称它是 In Profile 的。

Out of Profile：对于超出 QoS 监管策略规定范围（带宽或突发值）的流量，我们称它是 Out of Profile 的。

18.1.2 QoS 实现

对于 L3 交换机软件 QoS 的实现，首先应该给出一个参考模型，而这个模型要求是通用的、成熟的，下面将对 QoS 做一个尽量严格的描述：

IP 协议的数据传送规范，只针对发送端和接收端的地址和服务等作出规定，并且利用 OSI 四层以上的，如 TCP 协议等来确认数据包的传送正确无误，但是，IP 协议没有提供和保护传输数据包的带宽，而是以尽力而为（Best Effort）的方式来提供带宽服务。

此种方式对于 Mail 以及 FTP 等服务尚可以接收，但是对于越来越多的多媒体业务数据和电子商务数据的传输，则无法满足这些应用需要的带宽和低延迟要求。

QoS 并不能产生新的带宽，但是它可以将现有的带宽资源做一个最佳的调整和配置，完整的应用 QoS，可以对网络的数据传输做到完全的控管。

基于差别化服务的 QoS 在网络的入口指定每个数据包的优先级别，这些分类信息被携带在 L3 的 IP 包头或者 L2 的 802.1Q 帧头中。QoS 对于相同优先级别的数据包提供相同服务，而对不同级别的数据包则提供不同的操作。支持 QoS 的交换机或路由器可以根据数据包的分类信息，为其提供不同的带宽资源，并且可以根据配置的监管策略来重写这些数据包携带的分类信息甚至在带宽紧张的时候丢弃某些低级别的数据包。

如果在一个网络中，每一跳的设备都支持基于差别化服务的 QoS，那么就可以构建一个端到端的 QoS 解决方案。QoS 的配置是很灵活的，可以很复杂，也可以很简单，这一切都依赖于实际的网络拓扑和网络设备，以及对网络出入流量的分析。

18.1.3 QoS 基本模型

QoS 的基本模型分为五个部分：Classification（分类）、Policing（监管）、Mark（重写）、Queueing（整形）和 Scheduling（排程），其中分类、监管和重写是顺序执行的 QoS 的入口行为，整形和排程是 QoS 的出口行为。

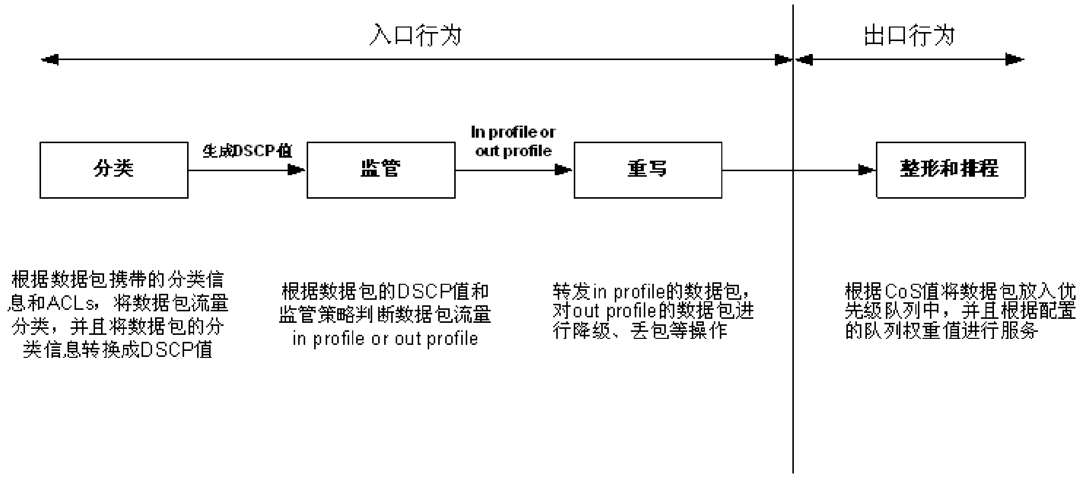


图 **1-3 QoS** 基本模型

分类：通过检查数据包的分类信息，来区别不同的流量，并且根据数据包的分类信息生成内部 DSCP 值。对于不同类型的数据包和不同的交换机配置，分类有不同的处理方式，由下面的流程图详细说明：

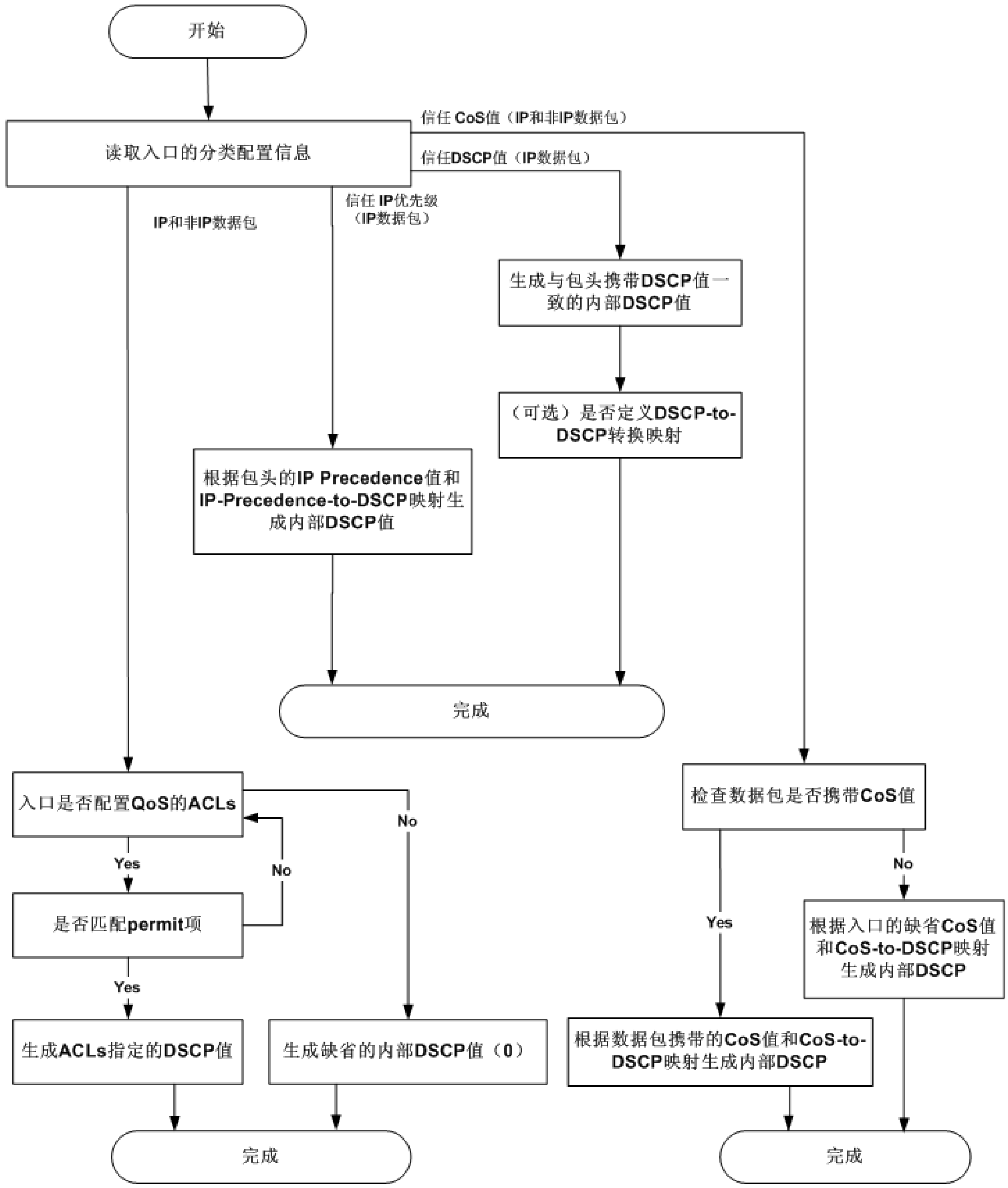


图 1-4 分类流程

监管和重写：在入口的流量经过分类，并且每个数据包都被分配了一个内部 DSCP 值以后，就可以进行监管和重写。

监管行为可以基于 DSCP 值配置不同的监管策略，为分类后的流量分配带宽，如果流量超过了监管策略规定的带宽，称为 out of profile，反之称为 in profile，对于 out of profile 的流量可以选择通过、丢包、重写三种处理方式；重写行为即用一个新的优先级别较低的 DSCP 值来代替数据包原有的级别较高的 DSCP 值，也称为 Marking Down。监管和重写的具体行为，由下面的流程图详细说明：

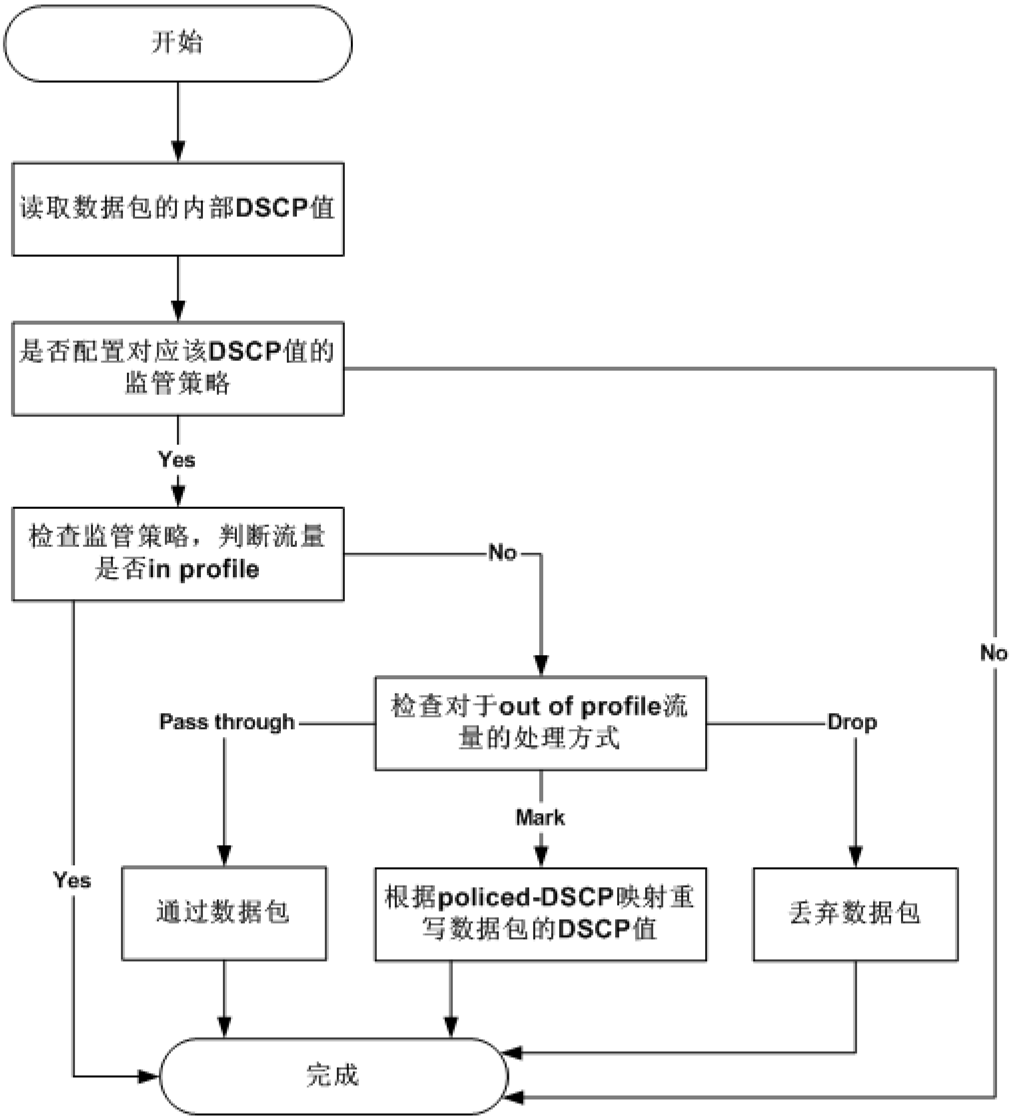


图 1-5 监管和重写流程

整形和排程：出口的数据包会将其携带的内部 DSCP 值重新映射成 CoS 值，整形行为根据数据包的 CoS 值将其分配到不同的优先级队列中；而排程行为则根据配置的优先级队列权重来进行数据包转发服务。整形和排程的具体行为，由下面的流程图详细说明：

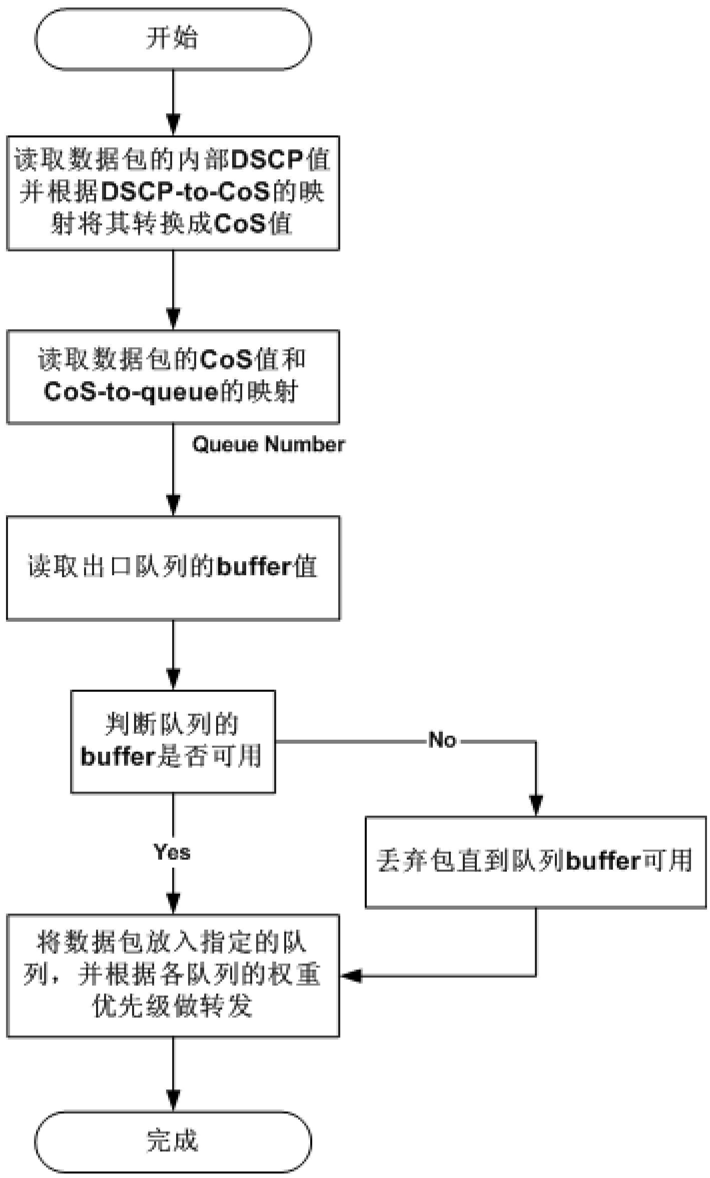


图 1-6 整形和排程流程

18.2 QoS 配置

18.2.1 QoS 配置任务序列

1. 启动 QoS 功能

在全局下启动和关闭 QoS 功能。必须在全局下启动 QoS 功能后才能配置其它的 QoS 命令。

2. 配置分类表（classmap）

建立一个分类规则，可以按照 ACL，VLAN ID，IP Precedent，DSCP 来分类。

3. 配置策略表（policymap）

建立一个策略表，可以对相应的分类规则

进行带宽限制，优先级降低等操作。

4．将 QoS 应用到端口

配置端口的信任模式，或者绑定策略。策略只有绑定到具体的端口，才在此端口生效。

5．配置出队队列工作方式和权重

将出队工作方式配置为 PQ 方式或者 WRR 方式，设置 4 个出口队列带宽的比例，以及内部优先级到出口队列的映射关系，都是全局命令，对所有端口生效。

6．配置 QoS 映射关系

配置 cos 到 dscp，dscp 到 cos，dscp mutation，ip precedent 到 dscp，policed-dscp 的映射关系。

1．启动 QoS 功能

命令	解释
全局配置模式	
mls qos **no mls qos**	启动和关闭 QoS 功能。

2．配置分类表（classmap）

命令	解释
全局配置模式	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	建立一个 class-map（分类表），并进入 class-map 模式；本命令的 no 操作为删除指定的 class-map。
match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| vlan <*vlan-list*>} **no match {access-group | ip dscp | ip precedence | vlan }**	设置分类表中的匹配标准；本命令的 no 操作为删除指定的匹配标准。

3．配置策略表（policymap）

命令	解释
全局配置模式	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	建立一个 policy-map（策略表），并进入 policy-map（策略表）模式；本命令的 no 操作为删除指定的 policy-map。
class <*class-map-name*> **no class <*class-map-name*>**	建立一个 class（策略分类表），并进入策略分类表模式；本命令的 no 操作为删除指定策略分类表。
set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>} **no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**	为分类后的流量分配一个新的 DSCP 和 IP Precedence 值；本命令的 no 操作为取消分配新的值。
police <*rate-bps*> <*burst-byte*> [exceed-action {drop |	为分类后的流量配置一个策略；本命令的 no 操作为删除指定的策略。

policed-dscp-transmit}] **no police <*rate-bps*> <*burst-byte*> [exceed-action {drop | policed-dscp-transmit}]**	
mls qos aggregate-policer <*aggregate-policer-name*> <*rate-bps*> <*burst-byte*> exceed-action {drop |policed-dscp-transmit} **no mls qos aggregate-policer <*aggregate-policer-name*>**	定义一个集合策略，这个策略可以在同一个策略表内部被多个策略分类表使用；本命令的 no 操作为删除指定的集合策略。
police aggregate <*aggregate-policer-name*> **no police aggregate <*aggregate-policer-name*>**	为分类后的流量应用一个集合策略；本命令的 no 为删除指定的集合策略。

4．将 QoS 应用到端口

命令	解释
接口配置模式	
mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]|ip-precedence [pass-through -cos]] **no mls qos trust**	配置交换机端口信任状态；本命令的 no 操作为禁止交换机端口的当前信任状态。
mls qos cos {<*default-cos*> } **no mls qos cos**	配置交换机端口的缺省 CoS 值；本命令的 no 操作为恢复缺省情况。
service-policy {input <*policy-map-name*> | output <*policy-map-name*>} **no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**	在端口上应用一个策略表；本命令的 no 操作为删除应用到交换机端口的某个指定策略表。
mls qos dscp-mutation <*dscp-mutation-name*> **no mls qos dscp-mutation <*dscp-mutation-name*>**	在端口上应用 DSCP 转换映射，本命令的 no 操作为恢复 DSCP 转换映射的缺省值。

5．配置出队队列工作方式和权重

命令	解释
全局配置模式	
wrr-queue bandwidth <*weight1 weight2 weight3 weight4*> **no wrr-queue bandwidth**	设置交换机所有端口出队列的 WRR 权重，本命令的 no 操作为恢复缺省值。
priority-queue out **no priority-queue out**	配置队列出队工作方式，将队列配置成 pq 出队工作方式，本命令的 no 命令为恢复 wrr 出队工作方式。
wrr-queue cos-map <*queue-id*> <*cos1* ...	设置 CoS 值对应交换机端口出队列的映

***cos8*>** **no wrr-queue cos-map [<*queue-id*>]**	射，本命令的 no 操作为恢复缺省值。

6．配置 QoS 映射关系

命令	解释
全局配置模式	
mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>} **no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**	设置 **CoS-to-DSCP** 映射，**DSCP-to-CoS** 映射，**DSCP-to-DSCP-mutation** 映射，**IP-precedence-to-DSCP** 映射和 **policed-DSCP** 映射；本命令的 no 操作为恢复缺省映射值。

18.2.2 QoS 配置命令

18.2.2.1 mls qos

命令：**mls qos**

no mls qos

功能：全局下启动 QoS；本命令的 no 操作为关闭全局的 QoS。

参数：无。

命令模式：全局配置模式

缺省情况：关闭 QoS。

使用指南：QoS 提供四个队列支持处理四种优先级别的流量。

举例：打开和关闭 QoS 功能。

Switch(config)#mls qos enable

Switch(config)#no mls qos enable

18.2.2.2 class-map

命令：**class-map <*class-map-name*>**

no class-map <*class-map-name*>

功能：建立一个 class-map（分类表），并进入 class-map 模式；本命令的 no 操作为删除指定的 class-map。

参数： **<*class-map-name*>** 分类表的名称。

缺省情况：缺省不存在分类表。

命令模式：全局配置模式

使用指南：

举例：创建和删除一个命名为 c1 的 class-map。

Switch(config)#class-map c1

Switch(config)#no class-map c1

18.2.2.3 match

命令：match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| vlan <*vlan-list*>}

no match {access-group | ip dscp | ip precedence | vlan }

功能：设置分类表中的匹配标准；本命令的 no 操作为删除指定的匹配标准。

参数：access-group <*acl-index-or-name*> 匹配指定的 ACL 表，参数为 ACL 的编号或名称；**ip dscp <*dscp-list*>** 匹配指定的 DSCP 值，参数为一个 DSCP 值列表，最多由 8 个 DSCP 值组成；**ip precedence <*ip-precedence-list*>** 匹配指定的 IP 优先级值，参数为一个 IP 优先级值列表，最多由 8 个 IP 优先级值组成，范围为 0～7；**vlan <*vlan-list*>** 匹配指定的 VLAN ID 值，参数为一个 VLAN ID 列表，最多 8 个 VLAN ID。

缺省情况：缺省不存在匹配标准。

命令模式：class-map（分类表）配置模式

使用指南：每个分类表内，只能设置一条匹配标准。

举例：创建一个命名为 c1 的 class-map，设置此 class-map 的分类规则是匹配 IP Precedenc 优先级为 0，1 的报文。

Switch(config)#class-map c1

Switch(config-ClassMap)#match ip precedence 0 1

Switch(config-ClassMap)#exit

18.2.2.4 policy-map

命令：policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

功能：建立一个 policy-map（策略表），并进入 policy-map（策略表）模式；本命令的 no 操作为删除指定的 policy-map。

参数：<*policy-map-name*> 策略表名称。

缺省情况：缺省不存在策略表。

命令模式：全局配置模式

使用指南：进入策略表配置模式后，可以进行一系列 QoS 的分类匹配和标记等操作。

举例：创建和删除一个命名为 p1 的 policy-map。

Switch(config)#policy-map p1

Switch(config)#no policy-map p1

18.2.2.5 class

命令：class <*class-map-name*>

no class <*class-map-name*>

功能：建立一个 class（分类表），并进入策略分类表模式；本命令的 no 操作为删除指定策略分类表。

参数：< *class-map-name* > 指定策略分类表采用的分类表名称。

缺省情况：缺省不存在策略分类表。

命令模式：策略表配置模式

使用指南：建立策略分类表以前，必须先建立一个策略表并且进入策略表模式；在策略分类表模式中，可以对按照分类表分类的包流量进行分类和策略配置，一个 policy-map 中最多只能配置 2 个 classmap。

举例：进入一个策略分类表模式。

Switch(config)#policy-map p1

Switch(config-PolicyMap)#class c1

Switch(config--Policy-Class)#exit

18.2.2.6 set

命令：set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}

no set {ip dscp | ip precedence}

功能：为分类后的流量分配一个新的 DSCP 和 IP Precedence 值；本命令的 no 操作为取消分配新的值。

参数：<*new-dscp*> 新的 DSCP 值；**<*new-precedence*>** 新的 IP 优先级值。

缺省情况：缺省不进行分配。

命令模式：策略分类表配置模式

使用指南：只有符合匹配标准被分类出来的流量才会被重新分配新的值。

举例：将满足 c1 分类规则的报文里的 IP Precedence 值都设为 3。

Switch(config)#policy-map p1

Switch(config-PolicyMap)#class c1

Switch(config--Policy-Class)#set ip precedence 3

Switch(config--Policy-Class)#exit

Switch(config-PolicyMap)#exit

18.2.2.7 police

命令：police <*rate-bps*> <*burst-byte*> [exceed-action {drop | policed-dscp-transmit}]

no police <*rate-bps*> <*burst-byte*> [exceed-action {drop | policed-dscp-transmit}]

功能：为分类后的流量配置一个策略；本命令的 no 操作为删除指定的策略。

参数：<*rate-bps*> 分类后的流量的平均波特率，单位是比特/秒，范围是 1000000～1000000000；**<*burst-byte*>** 分类后流量的突发值，单位是字节，范围是 1000～1000000；**exceed-action drop** 当超出指定的速率时，采取丢包的策略；**exceed-action policed-dscp-transmit** 当超出指定的速率时，采取 **mark down** 包 DSCP 值的策略。

缺省情况：缺省没有策略。

命令模式：策略分类表配置模式

使用指南： ***<rate-bps> <burst-byte>*** 值的范围很大，如果配置超过了端口的实际速率，应用这条策略的策略表就不会被捆绑到交换机端口。

举例：将满足 c1 分类规则的报文的带宽设置为 20M 比特/秒，突发值设置为 20K 字节，超出此带宽的报文一律丢弃。

```
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#police 20000000 20000 exceed-action drop
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
```

18.2.2.8 mls qos aggregate-policer

命令：mls qos aggregate-policer <*aggregate-policer-name*> <*rate-bps*> <*burst-byte*> exceed-action {drop |policed-dscp-transmit}

no mls qos aggregate-policer <*aggregate-policer-name*>

功能：定义一个集合策略，这个策略可以在同一个策略表内部被多个策略分类表使用；本命令的 no 操作为删除指定的集合策略。

参数：***<aggregate-policer-name>*** 集合策略的名称；***<rate-bps>*** 分类后的流量的平均波特率，单位是比特/秒，范围是 1000000～1000000000；***<burst-byte>*** 分类后流量的突发值，单位是字节，范围是 1000～1000000；**exceed-action drop** 当超出指定的速率时，采取丢包的策略；**exceed-action policed-dscp-transmit** 当超出指定的速率时，采取 **mark down** 包 DSCP 值的策略。

缺省情况：缺省没有定义集合策略。

命令模式：全局配置模式

使用指南：如果一个集合策略被某个策略表所采用，不能直接删除，必须先在对应的策略表内用 **no police aggregate <*aggregate-policer-name*>**命令取消对这个集合策略的引用，才能在全局模式下用 **no mls qos aggregate-policer <*aggregate-policer-name*>**删除该集合策略。

举例：将创建一个集合策略 aggregate-policer，命名为 agg1，此集合策略的定义为报文带宽设置为 20M 比特/妙，突发值设置为 20K 字节，超出此带宽的报文一律丢弃。

```
Switch(config)#mls qos aggregate-policer agg1 20000000 20000 exceed-action drop
```

18.2.2.9 police aggregate

命令：**police aggregate <*aggregate-policer-name*>**

no police aggregate <*aggregate-policer-name*>

功能：为分类后的流量应用一个集合策略；本命令的 no 为删除指定的集合策略。

参数：***<aggregate-policer-name>*** 集合策略的名称。

缺省情况：缺省没有定义集合策略。

命令模式：策略分类表配置模式

使用指南：可以在不同策略分类表内引用同一个集合策略。

举例：将满足 c1 分类规则的报文应用集合策略 agg1。

```
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#police aggregate agg1
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
```

18.2.2.10 mls qos trust

命令：mls qos trust {cos [pass-through-dscp] | dscp [pass-through-cos] | ip-precedence [pass-through-cos] | port priority <*priority*> }

no mls qos trust

功能：配置交换机端口信任状态；本命令的 no 操作为禁止交换机端口的当前信任状态。

参数：cos 配置端口信任 CoS 值；**cos pass-through-dscp** 配置端口信任 CoS 值但是不更改包的 DSCP 值；**dscp** 配置端口信任 DSCP 值；**dscp pass-through-cos** 配置端口信任 DSCP 值但是不更改包的 CoS 值；**ip-precedence** 配置端口信任 IP 优先级；**ip-precedence pass-through-cos** 配置端口信任 IP 优先级但是不更改包的 CoS 值；**port priority <*priority*>** 配置端口信任端口优先级，不更改包的 CoS 值。

缺省情况：不信任任何值。

命令模式：端口配置模式

使用指南：对于同时具有 CoS 值和 DSCP 值的包，如果不希望在 Classification 后，不被信任的那个值被更改，使用 **pass-through** 关键字进行保护。百兆以太网每 8 个端口是一个 Block，共有 3 个 Block，1-8 端口，9-16 端口，17-24 端口，千兆以太网每个端口是一个 Block，25 端口，26 端口；若是配置信任 DSCP，则以一个 Block 为单位，即在一个端口配置，本端口所在的 block 都有效。

举例：在端口 ethernet 0/0/1 配置信任 cos 值，即报文按 cos 值分类，同时不改变报文里的 DSCP 值。

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#mls qos trust cos pass-through-dscp
```

18.2.2.11 mls qos cos

命令：mls qos cos {<*default-cos*> }

no mls qos cos

功能：配置交换机端口的缺省 CoS 值；本命令的 no 操作为恢复缺省情况。

参数：<*default-cos*> 交换机端口的缺省 CoS 值，范围为 0～7。

缺省情况：缺省 CoS 值为 0。

命令模式：接口配置模式

使用指南：

举例：在端口 ethernet 0/0/1 配置缺省 cos 值为 5，即从此端口进来的报文如果不带 cos 值，

则分配默认 cos 值为 5。
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#mls qos cos 5

18.2.2.12 service-policy

命令：service-policy {input <*policy-map-name*> | output <*policy-map-name*>}
no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}
功能：在交换机端口上应用一个策略表；本命令的 no 操作为删除应用到交换机端口的某个指定策略表。
参数：input <*policy-map-name*> 将指定名称的策略表应用到交换机端口的入口；**output <*policy-map-name*>**将指定名称的策略表应用到交换机端口的出口。
缺省情况：缺省端口没有捆绑策略表。
命令模式：接口配置模式
使用指南：配置端口的信任状态和在端口上应用策略表是互斥的，较后的配置会覆盖以前的配置；每个端口在每个方向上只能应用一个策略表。目前在出口不支持出口策略表。
举例：在端口 ethernet 0/0/1 的入口上绑定策略 p1。
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)# service-policy input p1

18.2.2.13 mls qos dscp-mutation

命令：mls qos dscp-mutation <*dscp-mutation-name*>
no mls qos dscp-mutation <*dscp-mutation-name*>
功能：在交换机端口上应用 DSCP 转换映射，本命令的 no 操作为恢复 DSCP 转换映射的缺省值。
参数：<*dscp-mutation-name*> DSCP 转换映射的名称。
缺省情况：缺省没有 DSCP 转换映射。
命令模式：接口配置模式
使用指南：在交换机端口配置 DSCP 转换映射，该端口的信任状态必须为 trust DSCP 才会生效，应用 DSCP 转换映射，可以使指定 DSCP 值不经过 class 和 policy 直接转换为新的 DSCP 值；应用到千兆端口的 DSCP 转换映射只对本端口有效；应用到百兆端口的 DSCP 转换映射则存在一个作用范围，如果在 1～8 号端口中的某个端口应用 DSCP 转换映射，这个 DSCP 转换映射对于 1～8 号端口同时有效，在 9～16 号端口中的某个端口应用 DSCP 转换映射，它的作用范围是同时对 9～16 号端口有效，在 17～24 号端口中的某个端口应用 DSCP 转换映射，它的作用范围是同时对 17～24 号端口有效。
举例：在端口 ethernet 0/0/1 上配置信任 DSCP，采用 mu1 的 DSCP 转换映射。
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#mls qos trust dscp pass-through cos
Switch(Config-Ethernet0/0/1)#mls qos dscp-mutation mu1

18.2.2.14 wrr-queue bandwidth

命令：**wrr-queue bandwidth <*weight1 weight2 weight3 weight4*>**
no wrr-queue bandwidth
功能：设置交换机所有端口出队列的 WRR 权重，本命令的 no 操作为恢复缺省值。
参数：**<*weight1 weight2 weight3 weight4*>** WRR 权重值，范围为 1～100。
缺省情况：缺省 weight1，weight2，weight3，weight4 为 25
命令模式：全局配置模式
使用指南：WRR 权重的绝对值是没有意义的，WRR 通过四个权重值的比率来分配带宽。
举例：将四个出队列的带宽比重设为 1:2:4:8。
Switch(Config)#wrr-queue bandwidth 1 2 4 8

18.2.2.15 priority-queue out

命令：**priority-queue out**
no priority-queue out
功能：配置队列出队工作方式，将队列配置成 PQ 出队工作方式，本命令的 no 命令为恢复 WRR 出队工作方式。
参数：无
缺省情况：非 priority-queue 模式。
命令模式：全局配置模式
使用指南：当采用 priority-queue 出队模式后，不再采用 WRR 加权算法来发生报文，而是当前队列的报文发生完毕以后才发送下一个队列的报文。
举例：将出队工作方式设置为 priority-queue 工作方式。
Switch(config)#priority-queue out

18.2.2.16 wrr-queue cos-map

命令：**wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>**
no wrr-queue cos-map [<*queue-id*>]
功能：设置交换机端口出队列于 CoS 值的映射，本命令的 no 操作为恢复缺省值。
参数：**<*queue-id*>**为出队列的 ID，范围为 1～4；**<*cos1 ... cos8*>** 映射到出队列的 CoS 值最多为 8 个，范围为 0～7。
缺省情况：

Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	Queue Selected
0,1	1
2,3	2
4,5	3
6,7	4

命令模式：全局配置模式
使用指南：全局 QoS 关闭时，所有的 CoS 值都映射到队列 1。
举例：将 cos 值为 2，3 的报文映射到出队队列 1。
Switch(config)#wrr-queue cos-map 1 2 3

18.2.2.17 mls qos map

命令：**mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>}**

no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}

功能：设置 **class of service(CoS)-to-Differentiated Services Code Point (DSCP)** 映射，**DSCP-to-CoS** 映射，**DSCP-to-DSCP-mutation** 映射，**IP-precedence-to-DSCP** 映射和 **policed-DSCP** 映射；本命令的 no 操作为恢复缺省映射值。

参数： **cos-dscp <*dscp1...dscp8*>** 定义 CoS 值到 DSCP 值的映射，**<*dscp1...dscp8*>** 为 8 个 DSCP 值分别对应 CoS 值的 0～7，每个 DSCP 值之间用空格隔开，DSCP 值的范围为 0～63； **dscp-cos <*dscp-list*> to <*cos*>** 定义 DSCP 值到 CoS 值的映射，**<*dscp-list*>** 为 DSCP 值的列表，最多容纳 8 个 DSCP 值，**<*cos*>**为列表中的 DSCP 值所对应的 CoS 值；**dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*>** 定义 DSCP 值到 DSCP 值的转换映射，**<*dscp-mutation-name*>** 为转换映射的名称，**<*in-dscp*>** 入 DSCP 值，最多有 8 个，每个 DSCP 值之间用空格隔开，DSCP 值的范围是 0～63，**<*out-dscp*>** 出 DSCP 值，只有一个，在入 DSCP 中定义的 8 个值将被转变成出 DSCP 值；**ip-prec-dscp <*dscp1...dscp8*>** 定义 IP 优先级到 DSCP 值的转换，**<*dscp1...dscp8*>**为 8 个 DSCP 值分别对应 IP 优先级值的 0～7，每个 DSCP 值之间用空格隔开，DSCP 值的范围为 0～63；**policed-dscp <*dscp-list*> to <*mark-down-dscp*>** 定义 DSCP **mark down** 映射，**<*dscp-list*>** 为 DSCP 值的列表，最多容纳 8 个 DSCP 值，**<*mark-down-dscp*>**为 **mark down** 以后的 DSCP 值。

缺省情况： 缺省映射值为：

Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-CoS Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS Value	0	1	2	3	4	5	6	7

Default IP-Precedence-to-DSCP Map

IP Precedence Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

dscp-mutation 和 **policed-dscp** 缺省没有配置

命令模式：全局配置模式

使用指南：在 **police** 命令中，可以设置超过规定平均速率或突发值的分类包流量进行 **mark down** 处理，**policed-dscp <*dscp-list*> to <*mark-down-dscp*>** 可以设置将这些包的 DSCP 值 **mark down** 为新的 DSCP 值。

举例：将 ***CoS-to-DSCP*** 的映射值由默认的 0 8 16 24 32 40 48 56 改为 0 1 2 3 4 5 6 7。

Switch(config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7

18.3 QoS 举例

案例 1：

启动 QoS 功能，将出口队列的权重改为 1:2:4:8，将端口 ethernet 0/0/1 配置成信任 cos 模式，但是不改变报文里的 DSCP 值，并且将此端口的默认 cos 值设为 5。

配置步骤如下：

```
Switch#config
Switch(config)#mls qos
Switch(config)#wrr-queue bandwidth 1 2 4 8
Switch(config)#interface ethernet 0/0/1
Switch(config-Ethernet0/0/1)#mls qos trust cos pass-through dscp
Switch(config-Ethernet0/0/1)#mls qos cos 5
```

配置结果：

全局启动了 QoS 功能，出口带宽的比例依次为 1:2:4:8。当从 ethernet 0/0/1 进来的报文带 cos 值时，根据 cos 值到出口队列的映射关系，cos 值 0－7 分别对应出口队列 1，1，2，2，3，3，4，4，放到不同的优先队列，如果进来的报文不带 cos 值，则将其 cos 值设为 5，根据对应关系，放入优先级队列 3。所有经过的报文不改变其携带的 DSCP 值。

案例 2：

在端口 ethernet 0/0/2 上，将属于网段 192.168.1.0 内的报文带宽限制为 10M 比特/秒，突发值设为 4K 字节，超过带宽的该网段内的报文一律丢弃。

配置步骤如下：

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(config-ClassMap)#match access-group 1
Switch(config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#police 10000000 4000 exceed-action drop
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 0/0/2
Switch(Config-Ethernet0/0/2)#service-policy input p1
```

配置结果：

先设置一个 ACL：1，匹配网段 192.168.1.0。全局启动 QoS 功能，创建一个 class-map：c1，在 class-map 中匹配 ACL1，再创建一个 policy-map：p1，在 P1 中引用 c1，设置对应的 police 来限制带宽和峰值。然后在端口 ethernet 0/0/2 应用此 policy-map。设置后，

网 段 192.168.1.0 内 的 报 文 带 宽 在 端 口 ethernet 0/0/2 上被限制为 2M 字节每秒，突发值为 4K 字节，超过带宽的该网段内的报文一律丢弃。

案例 3：

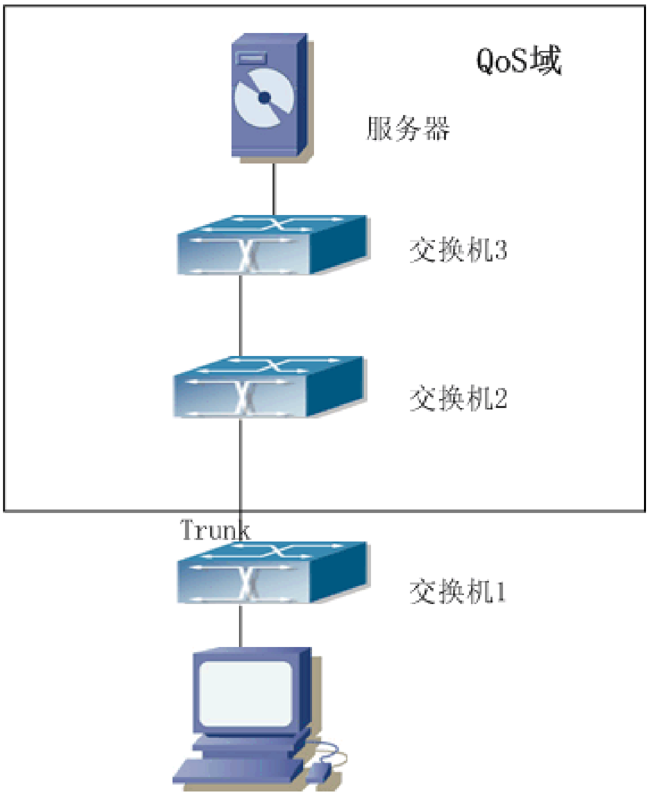


图 1-7

如图，方框内组成一个 QoS 域，交换机 1 将不同的流量分类，分配不同的 cos 优先级，如在端口 ethernet 0/0/1 上将属于网段 192.168.1.0 内的报文的 cos 优先级设为 5，与交换机 2 相连的端口为 trunk 口。在交换机 2 上，将与交换机 1 相连的端口 ethernet 0/0/1，设置信任 cos 优先级。这样在 QoS 域的内部，不同优先级的报文就走不同的队列，分配不同的带宽。

配置步骤如下：

交换机 **1** 上的 **QoS** 配置：

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(config-ClassMap)#match access-group 1
Switch(config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#set ip precedence 5
Switch(config--Policy-Class)#exit
```

Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#service-policy input p1
交换机 2 上的 QoS 配置：
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 0/0/1
Switch(config-Ethernet0/0/1)#mls qos trust cos pass-through dscp

18.4 QoS 排错帮助

18.4.1 QoS 调试和监测命令

18.4.1.1 show mls-qos

命令：**show mls-qos**
功能：显示 QoS 的全局配置信息。
参数：无。
缺省情况：无。
命令模式：特权用户配置模式
使用指南：
举例：
Switch #show mls-qos
Qos is enabled

显示内容	解释
Qos is enabled	Qos 功能打开

18.4.1.2 show mls qos aggregate-policer

命令：**show mls qos aggregate-policer [<*aggregate-policer-name*>]**
功能：显示 QoS 的集合策略配置信息。
参数：**<*aggregate-policer-name*>** 集合策略名称。
缺省情况：无。
命令模式：特权用户配置模式
使用指南：
举例：
Switch #show mls qos aggregate-policer policer1
aggregate-policer policer1 8000000 8000 exceed-action drop
Not used by any policy map

显示内容	解释

aggregate-policer policer1 8000000 8000 exceed-action drop	此集合策略的配置
Not used by any policy map	此集合策略被引用的次数

18.4.1.3 show mls qos interface

命令：show mls qos interface [<*interface-id*>] [buffers | policers | queueing | statistics]
功能：显示 QoS 在交换机端口上的配置信息。
参数：<*interface-id*>交换机端口 ID；**buffers：**端口的队列 buffer 设置；**policers：**端口的策略设置；**queueing：**端口的队列设置；**statistics：**端口对绑定策略的限制带宽内和带宽外分别通过的包个数。
缺省情况：无。
命令模式：特权用户配置模式
使用指南：只有配置入口策略时，才有统计信息。如果一个 Block 内的 8 个端口的入口策略配置相同，那么就显示 8 个端口的统计；否则显示单个端口的统计。
举例：
Switch #show mls qos interface ethernet 0/0/2
Ethernet0/0/2
default cos:0
DSCP Mutation Map: Default DSCP Mutation Map
Attached policy-map for Ingress: p1

显示内容	解释
Ethernet0/0/2	端口名
default cos:0	端口的默认 cos 值
DSCP Mutation Map: Default DSCP Mutation Map	端口的 DSCP 映射表名
Attached policy-map for Ingress: p1	端口绑定的策略名

Switch # show mls qos interface buffers ethernet 0/0/2
buffer size of 4 queue:256 256 256 256

显示内容	解释
buffer size of 4 queue:256 256 256 256	端口的 4 个出队列 可用的 buf 数目，固定设置，不可改变

Switch # show mls qos interface queueing ethernet 0/0/2
Ethernet0/0/2
Egress expedite queue: disable
wrr bandwidth weights:
1 1
2 2

3　4
4　8
Cos-queue map:
0　1
1　1
2　2
3　2
4　3
5　3
6　4
7　4

显示内容	解释
Ethernet0/0/2	端口名
Egress expedite queue: disable	是否设置了 priority-queue out 出队方式
wrr bandwidth weights: 1　1 2　2 3　4 4　8	4 队列分别对应的权重值
Cos-queue map: 0　1 1　1 2　2 3　2 4　3 5　3 6　4 7　4	Cos 值到 queue 的映射

Switch # show mls qos interface queueing ethernet 0/0/2
Ethernet0/0/2
Attached policy-map for Ingress: p1

显示内容	解释
Ethernet0/0/2	端口名
Attached policy-map for Ingress: p1	端口绑定的 policy-map

Switch # show mls qos interface statistics ethernet 0/0/2
Device: Ethernet0/0/2
Classmap　classified　in-profile　out-profile (in packets)
c1　0　0　0

显示内容	解释

Ethernet0/0/2	端口名
ClassMap	ClassMap 的名字
classified	匹配此 ClassMap 的数据报文总数
in-profile	匹配此 ClassMap 的 in-profile 数据报文总数
out-profile	匹配此 ClassMap 的 out-profile 数据报文总数

18.4.1.4 show mls qos maps

命令：show mls qos maps [cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp]

功能：显示 QoS 的映射配置信息。

参数：**cos-dscp** CoS 值到 DSCP 值的映射；**dscp-cos** DSCP 值到 CoS 值的映射；**dscp-mutation <*dscp-mutation-name*>** DSCP 值到 DSCP 值的转换映射，**<*dscp-mutation-name*>** 为转换映射的名称；**ip-prec-dscp** IP 优先级到 DSCP 值的转换；**policed-dscp** DSCP **mark down** 映射。

缺省情况：无。

命令模式：特权用户配置模式。

使用指南：

举例：

```
Switch # show mls qos map
    Cos-dscp map:
            cos:    0   1   2   3   4   5   6   7
    -------------------------------------
           dscp:    0   8 16 24 32 40 48 56


    IpPrecedence-dscp map:
         ipprec:    0   1   2   3   4   5   6   7
    -------------------------------------
           dscp:    0   8 16 24 32 40 48 56


    Dscp-cos map:
          d1 : d2 0   1   2   3   4   5   6   7   8   9
          0:        0   0   0   0   0   0   0   0   1   1
          1:        1   1   1   1   1   1   2   2   2   2
          2:        2   2   2   2   3   3   3   3   3   3
          3:        3   3   4   4   4   4   4   4   4   4
          4:        5   5   5   5   5   5   5   5   6   6
          5:        6   6   6   6   6   6   7   7   7   7
          6:        7   7   7   7
```

Policed-dscp map:

```
d1 : d2 0   1   2   3   4   5   6   7   8   9
0:       0   1   2   3   4   5   6   7   8   9
1:      10 11 12 13 14 15 16 17 18 19
2:      20 21 22 23 24 25 26 27 28 29
3:      30 31 32 33 34 35 36 37 38 39
4:      40 41 42 43 44 45 46 47 48 49
5:      50 51 52 53 54 55 56 57 58 59
6:      60 61 62 63
```

18.4.1.5 show class-map

命令：**show class-map [<*class-map-name*>]**
功能：显示 QoS 的分类表信息
参数：**<*class-map-name*>** 分类表名称
缺省情况：无
命令模式：特权用户配置模式
使用指南：
举例：
Switch # show class-map
Class map name:c1
Match acl name:1

显示内容	解释
Class map name:c1	ClassMap 的名字
Match acl name:1	ClassMap 的分类规则

18.4.1.6 show policy-map

命令：**show policy-map [<*policy-map-name*>]**
功能：显示 QoS 的策略表信息
参数：**<*policy-map-name*>** 策略表名称。
缺省情况：无。
命令模式：特权用户配置模式
使用指南：
举例：
Switch # show policy -map
Policy Map p1
Class Map name: c1
police 16000000 2000 exceed-action drop

显示内容	解释
Policy Map p1	policy-map 的名字
Class map name:c1	引用的 ClassMap 的名字
police 16000000 8000 exceed-action drop	采用的策略

18.4.2 QoS 排错帮助

- 交换机端口缺省关闭 QoS，缺省设置 4 条发送队列，队列 1 采用 best-effort（尽力而为）的方式转发普通的数据包，队列 4 发送一些重要的控制报文（BPDU 等）。
- 在使能全局 QoS 后，所有交换机端口打开 QoS 功能，设置 4 条发送队列。端口的缺省 CoS 值为 0，且关闭 CoS Override；端口为 not Trusted（不信任）状态；缺省每个优先级队列的 weights 值都为 25，所有的 QoS Map 都采用缺省值。
- CoS 值 7 默认映射到最高优先级队列 4，通常保留给某些协议报文使用，建议用户不要随意改变 COS 值 7 到队列 4 的映射关系，端口的缺省 CoS 值通常也不要设置为 7。
- 目前策略表只支持绑定到入口，对出口不支持。
- 由于某些时候受硬件资源的限制，如果策略过于复杂导致配置不成功时，会提示用户相关信息。

第19章L3 转发配置

三层转发是将三层协议报文（IP 报文）跨越 VLAN 进行转发，这种转发是用 IP 地址寻址的，当交换机的一个接口接收到 IP 报文后，会根据自己的路由表进行检索，然后根据结果决定对数据报文的操作，如果 IP 报文的目的地址是本交换机可达的另一个子网，那么就将此报文从交换机的相应接口发送出去。交换机可以使用硬件对 IP 报文进行转发，转发芯片中有相应的主机路由表和缺省路由表，其中，主机路由表用来存储与交换机直接相连的主机的路由，缺省路由表存储（经聚合算法计算后的）网段路由。

当单播流量转发需要的路由（主机路由或网段路由）在转发芯片中存在了，流量的转发就完全由硬件负责，而不像路由器那样还是 CPU 负责，因此大大提升了转发效率，可以达到线速转发。

19.1.1 三层接口

19.1.1.1 三层接口介绍

在 DCRS-5526S 交换机上可以创建三层接口。三层接口并不是实际的物理接口，它是一个虚拟的接口。三层接口是在 VLAN 的基础上创建的。三层接口可以包含一个或多个二层接口（它们同属于一个 VLAN），但也可以不包含任何二层接口。三层接口包含的二层接口中，需要至少有一个是 UP 状态，三层接口才是 UP 状态，否则为 DOWN 状态。每一个三层接口有自己独立的 MAC 地址，此地址是在三层接口创建时从交换机保留的 MAC 地址中选取的。三层接口是三层协议的基础，在三层接口上可以配置 IP 地址，交换机可以通过配置在三层接口上的 IP 地址，与其它设备进行 IP 协议的传输。交换机也可以在不同的三层接口之间转发 IP 协议报文。

19.1.1.2 三层接口配置

19.1.1.2.1三层接口配置任务序列

1. 创建三层接口

1.创建三层接口

命令	解释
全局配置模式	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	创建一个 VLAN 接口,（VLAN 接口属于三层接口）；本命令的 no 操作为删除交换机创建的 VLAN 接口（三层接口）。
接口配置模式	

Switchport no switchport	将创建的一个三层接口转变为交换机的二层接口；本命令的 no 操作为将交换机的二层接口转变为一个三层接口。

19.1.1.2.2三层接口配置命令

19.1.1.2.2.1 interface vlan

命令：interface vlan <*vlan-id*>
no interface vlan <*vlan-id*>

功能：创建一个 **VLAN** 接口，即创建一个交换机的三层接口；本命令的 no 操作为删除交换机的三层接口。

参数：<*vlan-id*> 是已建立的 VLAN 的 VLAN ID。

缺省情况：出厂时没有三层接口。

命令模式：全局配置模式

使用指南：在创建 VLAN 接口（三层接口）前，需要先配置 VLAN，详细内容参见 VLAN 的章节。使用本命令在创建 VLAN 接口（三层接口）的同时，进入 VLAN（三层接口）配置模式。在 VLAN 接口（三层接口）创建好之后，仍旧可以使用 interface vlan 命令进入三层接口模式。

举例：在 VLAN 1 上创建一个 VLAN 接口（三层接口）

Switch (Config)#interface vlan 1

19.1.1.2.2.2 switchport

命令：switchport
no switchport

功能：将创建的一个三层接口转变为交换机的二层接口；本命令的 no 操作为将交换机的二层接口转变为一个三层接口。

缺省情况：出厂时所有接口都是二层接口。

命令模式：接口配置模式

使用指南：三层接口必须以 VLAN 为基础，在使用本命令创建三层接口时，系统会从保留的 VLAN ID 中选取一个，来创建一个 VLAN，并将此接口置于这个 VLAN 中。在接口配置模式下，既有三层接口命令，也有二层接口命令，在接口转变为三层接口之前，三层命令的配置是无效的，但是在接口转变为三层接口后，原有的二层接口命令仍然有效。

举例：将接口 Ethernet 0/0/5 转变为一个三层接口

Switch (Config)#interface ethernet0/0/5
Switch(Config-Ethernet0/0/5)#no switchport

19.1.2 IP 转发

19.1.2.1 IP 转发介绍

网关设备可以将 IP 协议报文从一个子网转发到另一个子网中，这种转发是通过路由寻径的。交换机的 IP 转发是由硬件协助完成的，可以达到端口的线速转发。同时还可以提供各种灵活的控制，对转发行为进行调整和监控。该交换机可以支持禁止或允许优化的聚合算法以调整交换芯片中网段路由表项的生成，查看 IP 转发的统计信息，监视 IP 报文的收发状况，以及查看硬件转发芯片的状况。

19.1.2.2 IP 路由聚合配置

19.1.2.2.1IP 路由聚合配置任务

1. 配置是否使用优化 IP 路由聚合算法

1.配置是否使用优化 IP 路由聚合算法

命令	解释
Ip fib optimize **no ip fib optimize**	配置交换机使用优化 IP 路由聚合算法；本命令的 no 操作为配置交换机不使用优化 IP 路由聚合算法。

19.1.2.2.2IP 路由聚合配置命令

19.1.2.2.2.1 ip fib optimize

命令：ip fib optimize

no ip fib optimize

功能：配置交换机使用优化 IP 路由聚合算法；本命令的 no 操作为配置交换机不使用优化 IP 路由聚合算法。

缺省情况：出厂时不使用优化 IP 路由聚合算法。

命令模式：全局配置模式

使用指南：该命令是为了实现对聚合算法的优化，优化方法为：如果路由表不具备缺省路由，根据被引用最多的下一跳构造一个虚拟缺省路由，以简化聚合的结果。使用该方式的好处：更有效的简化了聚合的结果。

举例：配置交换机不使用优化 IP 路由聚合算法

Switch (Config)# no ip fib optimize

19.1.2.3 IP 转发排错帮助

19.1.2.3.1监测和调试命令

19.1.2.3.1.1 show ip traffic

命令：**show ip traffic**
功能：显示 IP 数据包统计信息。
命令模式：特权用户配置模式
使用指南：显示 IP 及 ICMP 数据包的接收、发送等统计信息。
举例：

```
Switch #show ip traffic
IP statistics：
   Rcvd：     290 total, 44 local destination
              0 header errors, 0 address errors
              0 unknown protocol, 0 discards
   Frags：    0 reassembled, 0 timeouts
              0 fragment rcvd, 0 fragment dropped
              0 fragmented, 0 couldn't fragment, 0 fragment sent
   Sent：     0 generated, 0 forwarded
              0 dropped, 0 no route
ICMP statistics：
   Rcvd：     0 total 0 errors 0 time exceeded
              0 redirects, 0 unreachable, 0 echo, 0 echo replies
              0 mask requests, 0 mask replies, 0 quench
              0 parameter, 0 timestamp, 0 timestamp replies
   Sent：     0 total 0 errors 0 time exceeded
              0 redirects, 0 unreachable, 0 echo, 0 echo replies
              0 mask requests, 0 mask replies, 0 quench
              0 parameter, 0 timestamp, 0 timestamp replies
```

显示信息	解释
IP statistics：	IP 数据包的统计信息：
Rcvd： 290 total, 44 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	接收总量的统计及其中有多少到达本地、多少数据包的包头有错误、多少地址有错误、多少不明协议的数据包、多少丢包等的统计。
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	分段统计：重组多少数据包、超时的有多少、接收分段数、丢失分段数、多少不能分段、发送多少分段等。
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route	发送总量的统计及其中包括多少从本地产生的、多少是转发的、多少丢失的、多少没有路由的等。
ICMP statistics：	ICMP 数据包的统计信息：
Rcvd： 0 total 0 errors 0 time exceeded	接收 ICMP 数据包总量的统计及将这些

0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	ICMP 数据包进行分类，分类后的统计数据。
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	发送 ICMP 数据包总量的统计及将这些 ICMP 数据包进行分类，分类后的统计数据。

19.1.2.3.1.2 show l3-table

命令：show l3-table [l3|defip|intf]
功能：显示硬件路由表。
参数：l3 显示主机路由表；**defip** 显示网段路由表；**intf** 先是三层接口表。
命令模式：特权用户配置模式
使用指南：显示硬件转发芯片中 IP 单播路由表。
举例：

```
Switch #show l3-table
L3INTF Table: MAX SIZE 32, FREE ENTRY 30
INTF    MAC                  VID
================================================================
0       00-03-0F-01-0E-10    1
1       00-03-0F-01-0E-11    2


DEFIP Table: MAX SIZE 16, FREE ENTRY 0
INDEX   IPADDR        MASKLEN   MAC                  PORT   INTF   CPU
================================================================
0       128.0.0.0     1         00-00-00-00-00-00    27     0      1
1       15.0.0.0      8         00-00-00-00-00-00    27     1      1
2       14.0.0.0      8         00-00-00-00-00-00    27     1      1
3       13.0.0.0      8         00-00-00-00-00-00    27     1      1
4       12.0.0.0      8         00-00-00-00-00-00    27     1      1
5       15.1.0.0      16        00-00-00-00-00-00    27     1      1
6       14.1.0.0      16        00-00-00-00-00-00    27     1      1
7       13.1.0.0      16        00-00-00-00-00-00    27     1      1
8       12.1.0.0      16        00-00-00-00-00-00    27     1      1
9       11.1.0.0      16        00-00-00-00-00-00    27     1      1
10      192.168.1.0   24        00-00-00-00-00-00    27     0      1
```

11 200.1.1.0 24
00-00-00-00-00-00 27 1 1
12 15.1.1.0 24 00-00-00-00-00-00 27 1 1
13 14.1.1.0 24 00-00-00-00-00-00 27 1 1
14 13.1.1.0 24 00-00-00-00-00-00 27 1 1
15 100.1.1.0 24 00-00-00-00-00-00 27 1 1

L3IP Table: MAX SIZE 2048, FREE ENTRY 2045
INDEX IPADDR MAC PORT HIT D_HIT INTF
==
1 192.168.1.100 00-03-0F-00-00-10 12 1 1 0
2 200.1.1.1 00-03-0F-00-04-31 22 1 1 1

显示信息	解释
L3INTF Table: MAX SIZE 32, FREE ENTRY 30	三层接口表，最大多少项，空余多少项
INTF	三层接口标识
MAC	三层接口的 MAC 地址
VID	三层接口的 VLAN ID
DEFIP Table: MAX SIZE 16, FREE ENTRY 0	缺省路由表，最大多少项，空余多少项
INDEX	序号
IPADDR	路由的 IP 前缀
MASKLEN	路由的 IP 掩码
MAC	下一跳的 MAC 地址
PORT	下一跳的端口号
INTF	下一条的三层接口
CPU	是否交给 CPU 处理
L3IP Table: MAX SIZE 2048, FREE ENTRY 2045	主机路由表，最大多少项，空余多少项
INDEX	序号
IPADDR	目的主机的 IP 地址
MAC	下一跳的 MAC 地址
PORT	下一跳的端口号
HIT	主机路由源命中
D_HIT	主机路由目的命中
INTF	下一跳的三层接口

显示三层接口表
Switch #sh l3-table intf
L3INTF Table

INDEX: 0, VID: 1, MAC_ADDR: 00-03-0f-01-3c-71

显示信息	解释
INDEX	三层接口索引值
VID	三层接口的 Vlan ID
MAC_ADDR	三层接口的 MAC 地址

显示主机路由表

Switch #sh l3-table l3

L3 Table

HW_INDEX: 2240, IP_ADDR: 192.168.1.100, SRC_IP_ADDR: 0.0.0.0

FLAGS: 0xb, INTF: 0, IP_MASK: 0.0.0.0

IPMC_PTR: 0x0, MAC_ADDR: 00-03-0f-fe-39-13, PORT_TGID: 6

显示信息	解释
HW_INDEX	硬件索引值
IP_ADDR	目的 IP 地址
SRC_IP_ADDR	源 IP 地址
FLAGS	标志
INTF	三层接口
IP_MASK	掩码
IPMC_PTR	IP 组播指针
MAC_ADDR	下一跳 MAC 地址
PORT_TGID	输出端口或汇聚组

显示缺省路由表

Switch #sh l3-table defip

DEFIP Table

DEFIP_IP_ADDR: 2.0.0.0, DEFIP_SUB_LEN: 8

PATH_L3_INDEX: 7, DEFIP_INTF: 0

FLAGS: 0x0, INTF: 0, MAC_ADDR: 00-03-0f-01-3c-71, PORT_TGID: 13

显示信息	解释
DEFIP_IP_ADDR	路由网段前缀
DEFIP_SUB_LEN	路由掩码长度
PATH_L3_INDEX	主机路由表索引
DEFIP_INTF	缺省路由表的三层接口
FLAGS	标志
INTF	指向的主机路由表的三层接口
MAC_ADDR	下一跳 MAC 地址
PORT_TGID	输出端口或汇聚组

19.1.2.3.1.3 debug ip packet

命令：**debug ip packet**

no debug ip packet

功能：打开 IP 报文调试开关；本命令的 no 操作为关闭调试开关。
缺省情况：缺省 IP 数据包调试功能是关闭的。
命令模式：特权用户配置模式
使用指南：显示接收或发送的 IP 数据包的内容，包括：源地址、目的地址、字节数等。
举例：打开 IP 报文调试开关。
Switch #debug ip packet
IP PACKET： rcvd, src 1.1.1.1, dst 1.1.1.2, size 100

19.1.3 ARP

19.1.3.1 ARP 介绍

ARP（Address Resolution Protocol）地址解析协议，主要用于 IP 地址到以太网 MAC 地址的解析。ARP 也可以静态配置。此外，在某些应用中，可以配置代理 ARP。当交换机的接口收到某 ARP 请求，该请求的 IP 地址与接口地址在一个 IP 网段，但却不在同一物理网络中，此时该接口若启动了代理 ARP 的功能，接口会将自己的 MAC 地址作为 ARP 的回应，然后将收到的实际数据报文进行转发。启动该项功能可以使因为物理网络分离但属于同一 IP 网段的机器忽视物理网络分离的事实，经过具有代理 ARP 接口的转发像处在一个物理网络中。

19.1.3.2 ARP 配置

19.1.3.2.1ARP 配置任务序列

1.配置静态 ARP
2.配置代理 ARP

1. 配置静态 ARP

命令	解释
arp <*ip_address*> <*mac_address*> **no arp <*ip_address*>**	配置静态 ARP 表项；本命令的 no 操作为删除静态 ARP 表项。

2. 配置代理 ARP

命令	解释
ip proxy-arp **no ip proxy-arp**	打开以太口代理 ARP 的功能；本命令的 no 操作为关闭代理 ARP 的功能。

19.1.3.2.2ARP 转发配置命令

19.1.3.2.2.1 arp

命令：**arp <*ip_address*> <*mac_address*>**

no arp <*ip_address*>

功能：配置静态 ARP 表项；本命令的 no 操作为删除静态 ARP 表项。

缺省情况：缺省没有静态 ARP 表项。

命令模式：接口配置模式

使用指南：在交换机上可以配置静态 ARP 表项。

举例：在接口 vlan 1 配置静态 ARP。

Switch(Config-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34

19.1.3.2.2.2 ip proxy-arp

命令：**ip proxy-arp**

no ip proxy-arp

功能：打开以太口代理 ARP 的功能；本命令的 no 操作为关闭代理 ARP 的功能。

缺省情况：缺省代理 ARP 功能是关闭的。

命令模式：接口配置模式

使用指南：当交换机的接口收到某 ARP 请求，该请求的 IP 地址与接口地址在一个 IP 网段，但却不在同一物理网络中，此时该接口若启动了代理 ARP 的功能，接口会将自己的 MAC 地址作为 ARP 的回应，然后将收到的实际数据报文进行转发。启动该项功能可以使因为物理网络分离但属于同一 IP 网段的机器忽视物理网络分离的事实，经过具有代理 ARP 接口的转发像处在一个物理网络中。代理 ARP 在回应 ARP 请求之前，需要查找路由表，以确定目的网络是否可达，只有目的网络可达的 ARP 请求，才会回应 ARP 请求。注意：匹配了缺省路由的 ARP 请求不进行代理。

举例：打开 ethernet0/0/1 代理 ARP 的功能。

Switch (Config-Ethernet0/0/1)#ip proxy-arp

19.1.3.3 ARP 转发排错帮助

19.1.3.3.1监测和调试命令

19.1.3.3.1.1 show arp

命令：**show arp [<*ip-addr*>][<*vlan-id*>][<*hw-addr*>][type {static|dynamic}][count]**

功能：显示 ARP 映射表。

参数：**<*ip-addr*>**为显示指定 IP 地址的表项；**<*vlan-id*>**为显示指定 vlan 标识的表项；**<*hw-addr*>**为显示指定 Mac 地址的表项；**static** 为显示静态 ARP 表项；**dynamic** 为显示动态 ARP 表项；**count** 为显示 ARP 表项数量信息。

命令模式：特权用户配置模式

使用指南：显示当前 ARP 映射表的内容，如：
IP 地址，硬件地址，硬件类型，接口名等。**举例**：
Switch#sh arp
Total arp items is 1, the matched arp items is 1

Address	Hardware Addr	Interface	Port	Flag
2.2.2.66	00-10-00-00-00-C5	Vlan1	Ethernet0/0/13	Dynamic

显示信息	解释
Addrss	IP 地址，此为 2.2.2.66；
Hardware Address	硬件地址，此为 00-10-00-00-00-C5；
Interface	三层接口。此为建在 vlan1 上的三层接口
Port	二层接口
Flag	ARP 表项属性，Dynamic or Static

19.1.3.3.1.2 debug arp

命令：**debug arp**
no debug arp
功能：打开 ARP 调试开关；本命令的 no 操作为关闭该调试功能。
缺省情况：缺省 ARP 调试功能是关闭的。
命令模式：特权用户配置模式
使用指南：显示接收或发送的 ARP 数据包的内容，包括：类型、源地址、目的地址。
举例：打开 ARP 调试开关。
Switch #debug arp
ARP： rcvd, type 1, src 1.1.1.1 1234.1234.1234, dst 1.1.1.2 5678.5678.5678

19.1.3.3.2ARP 排错帮助

交换机无法 PING 通直接相连的网络设备，检查可能存在的情况和建议的解决方法：
☞ 首先检查交换机是否学习到相应的 ARP；
☞ 若 ARP 未能学习到，那么使用 ARP 的调试信息，观察 ARP 协议报文的收发情况；
交换机无法 PING 通直接相连的网络设备，检查可能存在的情况和建议的解决方法：

- 首先检查交换机是否学习到相应的 ARP；
- 若 ARP 未能学习到，那么使用 ARP 的调试信息，观察 ARP 协议报文的收发情况；
- 用户比较容易遇到的现象是线缆有问题，导致 ARP 不能学习。

第20章路由协议配置

在 Internet 网中，一台主机为了访问远端的另一台主机，必须通过一系列路由器或三层交换机选择一条合适的路径。

路由器或三层交换机都是通过 CPU 来计算路径，不同的是三层交换机将计算出来的路径添加到交换芯片中，由芯片进行线速转发；而路由器始是将计算出来的路径保存在路由表和路由缓存区中，由 CPU 负责数据转发。可见，路由器和三层交换机都可以进行路径的选择，而三层交换机在数据转发上有比较强大的优势。下面简单描述一下三层交换机的路径选取的基本原理和方法。

在路径选取过程中，每台三层交换机只负责根据收到数据包的目的地址来选择一条合适的中间路径，然后将数据包传送给下一个三层交换机，直至路径上的最后一台三层交换机将数据包传送给目的主机。每台三层交换机所完成的将数据包传送到下一个三层交换机而选择的路径，就被称作路由。路由可以分为直连路由、静态路由和动态路由等几种。

直连路由是指到与该三层交换机直接相连网络的路径，三层交换机不用计算就可以获得。

静态路由是指人为指定的到某个网络或特定主机的路径，静态即不能随意更改。静态路由的优点是简单易配、稳定、限制非法的路由改变，便于实现负载分担，便于实现路由备份。但是，因为是人为设置，对于大型网络需要设置的路由过于庞大和复杂，因此不适用于中大型网络。

动态路由是指三层交换机根据启动的路由协议动态计算到某个网络或特定主机的路径。如果路径中下一跳三层交换机不可达，三层交换机能够自动丢弃通过该三层交换机的路径，选择通过其它三层交换机的路径。

动态路由协议一般分为两类：内部网关路由协议（IGP）和外部网关路由协议（EGP）。内部网关路由协议（IGP）是用来计算到某个自治系统内目的路由的协议。神州数码三层交换机支持的内部网关动态路由协议有 RIP 和 OSPF 路由协议，可以根据需要配置 RIP 和 OSPF 路由协议。神州数码三层交换机支持同时运行多个内部网关动态路由协议，也可以在某个动态路由协议中重新引入其它动态路由协议和静态路由从而将多个路由协议联系起来。

20.1 路由表

如前所述，三层交换机主要用于建立当前三层交换机到达某个网络或特定主机的路由，并根据路由转发数据包。每台三层交换机都建立有一张路由表，记录着该三层交换机使用的所有路由。路由表中每条路由项都指明了数据包到某子网或主机应该通过三层交换机的哪个 vlan 接口发送，方可达到目的主机或到目的主机路径的下一台三层交换机。

路由表中包含下列一些主要的内容：

- 目的地址：用于标识 IP 数据包的目的地址或目的网络。
- 网络掩码：与目的地址一起标识目的主机或三层交换机所在网段的网段地址。网络掩码由若干个连续的“1”构成，通常以点分十进制标识（一般为 1 到 4 个 255 组成的地址）。将目的地址和网络掩码“与”之后，可以得到到目的主机或三层交换机所

在网段的网络地址。例如，目的地址
为 200.1.1.1，掩码为 255.255.255.0 的主机或三层交换机所在网段的网络地址为 200.1.1.0。

- 输出接口：指明 IP 数据包将从该三层交换机的哪个接口转发。
- 下一台三层交换机（下一跳）IP 地址：指明 IP 数据包将经由的下一台三层交换机。
- 路由项优先级：针对同一目的地，可能存在不同下一跳的若干条路由。这些路由可能是不同的动态路由协议发现的，也可能是人为配置的静态路由。优先级高的（数值小）将成为当前的最优路由。用户可以配置到同一目的地优先级不同的多条路由，三层交换机将按优先级顺序选取唯一的一条路由用于 IP 数据包转发。

为了不使路由表过于庞大，可以设置一条缺省路由。一旦查找路由表失败后，就选择缺省路由转发数据包。

三层交换机支持的各种路由协议及其发现路由的缺省优先级如下表表示：

路由协议或路由种类	优先级缺省值
直连路由	0
OSPF	110
静态路由（static）	1
RIP	120
OSPF ASE	150
IBGP	200
EBGP	20
未知路由	255

20.2 静态路由

20.2.1 静态路由介绍

如前所述，静态路由是指人为指定的到某个网络或特定主机的路径。静态路由的优点是简单易配、稳定、能够禁止非法的路由改变，同时便于实现负载分担和路由备份。但是，它也存在许多缺点。静态路由是静态的，一旦网络发生故障不能自动修改路由，必须人为参与配置，不适用于中大型网络。

静态路由主要应用于两种情况：1）对于稳固的网络，为减少路由选择和路由数据流的负载，可使用静态路由。例如，到 STUB 网络的路由可采用静态路由。2）为实现路由备份，可以使用静态路由（在备份线路配置静态路由，路由优先级低于主线路）。

静态路由与动态路由可以同时存在，三层交换机根据路由协议优先级的不同，选用优先级最高的路由。同时，在动态路由中也可以通过重新引入静态路由的方式（redistribute），将静态路由加入到动态路由中，并根据需要改变引入静态路由的优先级。

20.2.2 缺省路由介绍

缺省路由也是一种静态路由，它是在没有找到任何匹配路由时才使用的路由。在路由表中，缺省路由的表示形式为目的地址为 0.0.0.0，网络掩码也为 0.0.0.0 的路由。如果路由表

中没有数据包所要到达的目的地，也没有缺省
路由，则丢弃该数据包，并向源地址返回一个 ICMP 数据报指出此目的地址或网络的不可达。

20.2.3 静态路由配置

20.2.3.1 静态路由配置任务序列

1. 静态路由配置
2. 缺省路由配置

1.静态路由配置

命令	解释
全局配置模式	
ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>] **no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]**	配置静态路由；本命令的 no 操作为删除静态路由。

2.缺省路由配置

命令	解释
全局配置模式	
ip route 0.0.0.0 0.0.0.0 <*gateway*> [<*preference*>] **no ip route 0.0.0.0 0.0.0.0 <*gateway*> [<*preference*>]**	配置缺省路由；本命令的 no 操作为删除缺省路由。

20.2.3.2 静态路由配置命令

- **ip route**
- **show ip route**

20.2.3.2.1ip route

命令：**ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]**
no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]
功能：配置静态路由；本命令的 no 操作为删除静态路由。
参数：**<*ip_address*>**和**<*mask*>**分别为目的 IP 地址和子网掩码，点分十进制格式；**<*gateway*>**为下一跳的 IP 地址，点分十进制格式；**<*preference*>**为路由优先级，取值范围为 1～255，preference 的值越小优先级越高。
缺省情况：静态路由缺省优先级为 1。
命令模式：全局配置模式
使用指南：在配置静态路由的下一跳时，可采用指定路由数据包发送下一跳 IP 地址方式。

各种路由类型缺省的 preference 为：

路由类型	Preference 值
直连路由	0
静态路由	1
OSPF	110
RIP	120
IBEP	200
EBGP	20

在不改变各种路由优先级值的情况下，直连路由优先级最高，依次是静态路由、EBGP、OSPF、RIP、IBGP。

举例：

例 1．添加一条静态路由。

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

例 2．添加缺省路由。

Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

20.2.3.2.2 show ip route

命令：show ip route [dest <*destination*>] [mask <*destMask*>] [nextHop <*nextHopValue*>] [protocol {connected | static | rip| ospf | ospf_ase | bgp | dvmrp}] [<*vlan-id*>] [preference <*pref*>] [count]

功能：显示路由表。

参数：<***destination***>为目标网络地址；<***destMask***>为目标网络的掩码；<***nextHopValue***>为下一跳 IP 地址；**connected** 为直连路由；**static** 为静态路由；**rip** 为 RIP 路由；**ospf** 为 OSPF 路由；**ospf_ase** 为 OSPF 引入的路由；**bgp** 为 BGP 路由；**dvmrp** 为 DVMRP 路由；<***vlan-id***> 为 Vlan 标识符；<***pref***> 为路由优先级，取值范围为 0～255；**count** 为显示 IP 路由表项数量信息。

命令模式：特权用户配置模式

使用指南：显示核心路由表的内容，包括：路由类型、目的网络、掩码、下一跳地址、接口等。

举例：

```
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
        A - OSPF ASE, B - BGP derived

    Destination      Mask             Nexthop        Interface     Pref
C   2.2.2.0          255.255.255.0    0.0.0.0        vlan2         0
C   4.4.4.0          255.255.255.0    0.0.0.0        vlan4         0
S   6.6.6.0          255.255.255.0    9.9.9.9        vlan9         1
R   7.7.7.0          255.255.255.0    8.8.8.8        vlan8         120
```

显示信息	解释
C - connected	直连路由，即与三层交换机直接相连的网段；
S – static	静态路由，由用户手工配置的路由；
R - RIP derived	RIP 路由，三层交换机通过 RIP 协议得到的；

O - OSPF derived	OSPF 路由，三层交换机通过 OSPF 协议得到的；
A- OSPF ASE	OSPF 引入的路由
B- BGP derived	BGP 路由，路由通过 BGP 协议得到
Destination	目标网络；
Mask	目标网络的掩码；
Nexthop	下一跳 IP 地址；
Interface	下一跳经过的三层交换机接口；
Pref	路由的优先级，如果到达目标网络还有其它类型的路由，在核心路由表中只显示优先级高的路由信息。

20.2.4 配置案例

下图是由三台神州数码三层交换机组成的一个简单的网络，各三层交换机和 PC 机 IP 地址的网络掩码均为 255.255.255.0， SWITCH-1 与 SWITCH-3 之间都通过配置静态路由以使 PC1 和 PC3 之间进行通信，PC3 到 PC2 之间的通信通过在 SWITCH-3 上配置到 SWITCH-2 的静态路由来实现，PC2 到 PC3 之间的通信通过在 SWITCH-2 上配置缺省路由来实现。

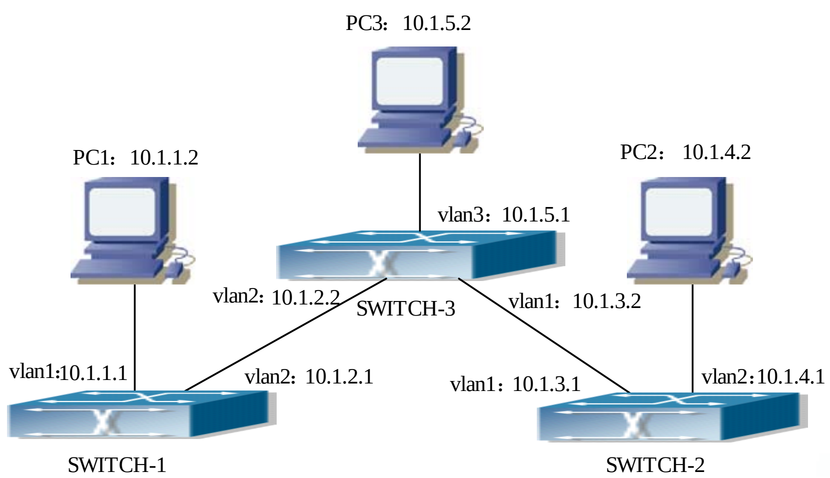


图 20-1 静态路由示意图

配置步骤：

三层交换机 SWITCH-1 的配置

Switch#config

Switch(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.2

三层交换机 SWITCH-3 的配置

Switch#config

！下一跳采用对端 IP 地址

Switch(config)#ip route 10.1.1.0
255.255.255.0 10.1.2.1
！下一跳采用对端 IP 地址
Switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1
三层交换机 SWITCH-2 的配置
Switch#config
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2
这样，PC1 与 PC3、PC2 与 PC3 之间都可以 PING 通。

20.2.5 排错帮助

20.2.5.1 监测和调试命令

命令	解释
特权模式	
show ip route	显示路由表的内容，包括：路由类型、目的网络、掩码、下一跳地址、接口等。

使用 show ip route 命令可以显示路由表中关于静态路由的目的 IP 地址、网络掩码以及下一跳 IP 地址或转发接口等信息。
例如：

```
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived

    Destination      Mask             Nexthop        Interface       Pref
C   2.2.2.0          255.255.255.0    0.0.0.0        vlan1           0
S   6.6.6.0          255.255.255.0    2.2.2.9        vlan1           1
```

其中，S 表示静态路由，即目的网络地址为 6.6.6.0、网络掩码为 255.255.255.0、下一跳地址为 2.2.2.9 以及转发接口为以太口 vlan1 的一条路由为静态路由，它的优先级为 1。

20.3 RIP

20.3.1 RIP 介绍

RIP协议最早在ARPANET网络中上使用，专门用于小型简单网络中。RIP协议是基于Bellman-Ford算法的距离向量路由协议。运行距离向量协议的网络设备定期向相邻设备发送两种信息：

- 到达目的网络所经过的跳数，即使用的度（metric），或者通过网络的数量。
- 下一个跳是什么，或者达到目的网络要使用的方向（向量）。

距离向量三层交换机定期向相邻的三层交换机发送它们的整个路由选择表。三层交换机在从相邻三层交换机接收到的信息的基础之上建立自己的路由选择信息表。然后，将信息传

递到它的相邻三层交换机。结果是路由选择表
是在第二手信息的基础上建立的，距离代价超过15跳的路由将被视为不可达。

RIP协议是可选路由协议，它是基于UDP的协议，使用RIP的每个主机在UDP的520端口上发送和接收数据报。所有运行RIP协议的三层交换机，每隔30秒向所有邻居三层交换机发送路由表更新信息。如果180秒内没有收到来自对端的信息，那么认为该设备崩溃或相连的网络不可达。但到该三层交换机的路由还将在路由表中保持120秒，然后才被删除。

由于运行RIP协议的三层交换机使用第二手信息建立路由表，因此至少会遇到一个问题——无穷记数问题。对于一个运行RIP路由协议的网络，当某条RIP路由变为不可达，RIP三层交换机通常不会立刻发送路由更新报文，而是等待到达周期更新时间间隔（每30秒）时才发送有该路由信息的更新数据报。如果在没有收到更新报文之前，邻居向该三层交换机发送了一个包含邻居三层交换机自身路由表信息的数据报，那么会引起"无穷记数"现象，即出现到不可达三层交换机的路由选择度量固定递增的现象。这大大影响了路由选择、路由汇聚时间。

为了避免"无穷记数"现象，RIP 协议提供了"水平分割"和"触发更新"等机制来解决路由循环问题。"水平分割"的原理是避免向网关发送从该网关学习到的路由，它包括"简单水平分割"——删除从邻居网关学习到的、将发送给该邻居网关的路由，和"逆向毒性水平分割"——不但在更新包中删除上述路由，而且将这些路由的代价设置为无穷。 "触发更新"机制定义无论网关何时改变路由度量，都立即将更新数据报并以广播形式发送出去，而不考虑 30 秒更新定时器的状态。

RIP 协议包含版本 1 和版本 2 两个版本：RFC1058 中介绍了 RIP-I 协议；RFC2453 中介绍了 RIP-II 协议，同时兼容 RFC1723 和 RFC1388。RIP-I 采用发送广播数据报的方式发送路由更新数据报，它不支持子网掩码和认证。RIP-I 的数据报中有一些域是不使用的，要求保证是全"0"，因此如果使用 RIP-I 应该进行全"0"域检查，如果这些域非"0"则丢弃此 RIP-I 数据报。RIP-II 版本比 RIP-I 版本完善，它采用发送组播数据报的方式发送路由更新数据报（组播地址为 224.0.0.9），它增加了子网掩码域和 RIP 验证域（支持简单明文密码和 MD5 密码验证），支持可变长子网掩码。RIP-II 使用了 RIP-I 中的部分全"0"域，因此无需进行全"0"域检查。DCRS 系列三层交换机缺省情况下是组播发送 RIP-II 数据报，接收 RIP-I 和 RIP-II 数据报。

每个运行 RIP 协议的三层交换机都有一个路由数据库，数据库中包含了该三层交换机所有可达目的地的路由项，并以此建立路由表。当 RIP 三层交换机向其相邻设备发送路由更新数据报时，路由更新数据报中包含了该三层交换机依据路由数据库建立的整个路由表。因此，对于较大的网络系统，每台三层交换机需要传输和处理的路由数据量很大、负担重，从而大大影响网络性能。

同时，RIP 协议支持将其它路由协议发现的路由信息引入到路由表中。

RIP 协议运行过程描述如下：

1. 启动 RIP，以广播形式向其相邻三层交换机发送请求数据报，相邻设备收到请求数据报后，响应该请求，并回送包含本地路由信息的响应数据报。
2. 三层交换机接收到响应数据报后，修改本地路由表，同时向相邻设备发送触发更新数据报，广播路由更新信息。相邻三层交换机接收到触发更新数据报之后，向其相邻的三层交换机发送触发更新数据报。经过一连串触发更新报的广播之后，各三层交换机都得到并保持最新的路由信息。

同时，RIP 三层交换机每隔 30 秒向其相邻设备广播本地路由表。相邻设备在接收到数据报之后，对本地路由进行维护，选择出最佳路由并向其各自的设备广播更新信息，使更新

的路由最终达到全局有效。另外，RIP 采用超
时机制对过时的路由进行超时处理，即三层交换机在一定时间间隔内（invalid 定时器间隔）没有收到来自某邻居的周期更新数据报，则认为来自该三层交换机的路由为无效路由，然后该路由再在路由表中保留一定时间间隔（holddown 定时器间隔），最后删除该路由。

20.3.2 RIP 配置

20.3.2.1 RIP 配置任务序列

1. 启动 RIP 协议（必须）
   （1）启动 RIP 模块/关闭 RIP 模块
   （2）配置接口使能发送/接收 RIP 数据报
2. 配置 RIP 协议参数（可选）
   （1）配置 RIP 发包机制
      1）配置 RIP 数据报的定点发送
      2）配置 RIP 广播
   （2）配置 RIP 路由参数
      1）配置路由聚合
      2) 配置引入路由（缺省路由权值、配置 RIP 中引入其它协议的路由）
      3）配置接口发送/接收 RIP 数据报的附加路由权值
      4）配置接口的验证模式及密码
   （3）配置 RIP 协议其它参数
      1）配置 RIP 路由优先级
      2）配置 RIP 数据报的零域检查
      3）配置 RIP 更新、超时、抑制等计时器时间
3. 配置 RIP-I/RIP-II 模式切换
   （1）配置所有接口使用的 RIP 版本
   （2）配置接口发送/接收的 RIP 版本
   （3）配置接口是否发送/接收 RIP 数据报
4. 关闭 RIP 协议

1.启动 RIP 协议

在神州数码三层交换机上运行 RIP 路由协议的基本配置很简单，通常只需打开 RIP 开关、使能发送和接收 RIP 数据报，即按 RIP 缺省配置发送和接收 RIP 数据报（缺省发送 RIP-II 接收 RIP-I 和 RIP-II）。如果需要可以切换发送、接收 RIP 数据报的版本，允许/禁止发送、接收 RIP 数据报，参考 3。

命令	解释
全局配置模式	
[no] router rip	打开 RIP 协议；本命令的 no 操作关闭 RIP 协议。
接口配置模式	

[no] ip rip work	设定在接口上发送并接收 RIP 数据报文；本命令的 no 操作为关闭本接口的 RIP 数据报文收发。

2.配置 RIP 协议参数

（1）配置 RIP 发包机制

1）配置 RIP 数据报的定点发送

2）配置 RIP 广播

命令	解释
RIP 协议配置模式	
[no] rip broadcast	指示 RIP 三层交换机允许所有接口发广播包或组播包；本命令的 no 操作禁止各端口发广播包或组播包。

（2）配置 RIP 路由参数

1) 配置路由聚合

命令	解释
RIP 协议配置模式	
auto-summary **no auto-summary**	配置路由聚合功能；本命令的 no 操作取消路由聚合功能。

2）配置引入路由（缺省路由权值、配置 RIP 中引入其它协议的路由）

命令	解释
RIP 协议配置模式	
default-metric <*value*> **no default-metric**	设定引入路由的缺省路由权值；本命令的 no 操作恢复缺省设置。
redistribute { static | ospf | bgp} [metric <*value*>] **no redistribute { static | ospf | bgp }**	在 RIP 数据报中引入静态、OSPF 协议或 BGP 协议的路由；本命令的 no 操作取消引入的相应协议的路由。

3）配置接口发送/接收 RIP 数据报的附加路由权值

命令	解释
接口配置模式	
ip rip metricout <*value*> **no ip rip metricout**	设定接口发送 RIP 数据报时给路由增加的附加路由权值；本命令的 no 操作恢复缺省发送附加路由权值配置。
ip rip metricin <*value*> **no ip rip metricin**	设定接口接收 RIP 数据报时给路由增加的附加路由权值；本命令的 no 操作恢复缺省接收附加路由权值配置。

4）配置接口的验证模式及密码

命令	解释

接口配置模式	
ip rip authentication mode {text| md5 type {cisco|usual}} **no ip rip authentication mode**	设置验证使用的类型；本命令的 no 操作设置为缺省值，即使用文本验证。
ip rip authentication key-chain <*name-of-chain*> **no ip rip authentication key-chain**	设置验证使用的密钥；本命令的 no 操作设成不使用验证密钥。

（3）配置 RIP 协议其它参数

1）配置 RIP 路由优先级

2）配置 RIP 数据报的零域检查

3）配置 RIP 更新、超时、抑制等计时器时间

命令	解释
RIP 协议配置模式	
rip preference <*value*> **no rip preference**	指定 RIP 协议的路由优先级；本命令的 no 操作恢复缺省值。
[no] rip checkzero	使能对 RIP-I 数据报的零域进行检查，零域的值不为零则拒绝处理；本命令的 no 操作取消对零域的查零操作。
timer basic <*update*> <*invalid*> <*holddown*> **no timer basic**	调整 RIP 计时器 更新、期满、抑制的时间；本命令的 no 操作回复缺省设置。

3. 配置 RIP-I/RIP-II 模式切换

（1）配置所有接口使用的 RIP 版本

命令	解释
RIP 协议配置模式	
version { 1 | 2 } **no version**	设置所有三层交换机接口发送/接收 RIP 数据报的版本；no 操作恢复缺省设置，即发送版本 2，接收版本 1 和 2 的数据报。

（2）配置接口发送/接收的 RIP 版本？

（3）配置接口是否发送/接收 RIP 数据报

命令	解释
接口配置模式	
ip rip send version { v1 | v2 [bc|mc] } **no ip rip send version**	设置接口发送 RIP 数据报版本；本命令的 no 操作恢复缺省设置，即发送版本 2。
ip rip receive version {v1 | v2 | v12} **no ip rip receive version**	设置接口接收 RIP 数据报版本；本命令的 no 操作恢复缺省设置，即接收版本 1 和版本 2 的 RIP 数据报。
[no] ip rip input	设定在接口上接收 RIP 数据报；本命令的 no 操作，关闭本接口的 RIP 数据报接收。

[no] ip rip output	设定在接口上发送 RIP 数据报；本命令的 no 操作，关闭本接口的 RIP 数据报发送。

4. 关闭 RIP 协议

命令	解释
全局配置模式	
no router rip	关闭 RIP 路由协议。

RIP（Routing Information Protocol）路由信息协议，是基于距离矢量的动态内部路由协议，由于配置较简单，所以应用很广泛。RIP 通过广播 UDP 报文来交换路由信息，每 30 秒发一次路由更新信息。它以跳数作为选取路由的标准，到同一目标网络优先选取跳数最小的路由路径。跳数的最大值为 16，所以 RIP 适用于直径较小的自治系统。RIP 的配置命令主要是在全局配置模式、RIP 协议配置模式、接口配置模式和特权用户配置模式下进行。

20.3.2.2 RIP 的配置命令

- **auto-summary**
- **default-metric**
- **ip rip authentication key-chain**
- **ip rip authentication mode**
- **ip rip metricin**
- **ip rip metricout**
- **ip rip input**
- **ip rip output**
- **ip rip receive version**
- **ip rip send version**
- **ip rip work**
- **ip split horizon**
- **redistribute**
- **rip broadcast**
- **rip checkzero**
- **rip preference**
- **router rip**
- **timer basic**
- **version**
- **show ip protocols**
- **show ip rip**
- **debug ip rip packet**
- **debug ip rip recv**
- **debug ip rip send**

20.3.2.2.1auto-summary

命令：**auto-summary**

no auto-summary

功能：配置路由聚合功能，本命令的 no 操作取消路由聚合功能。

参数：无

缺省情况：不使用自动路由聚合功能

命令模式：RIP 协议配置模式

使用指南：路由聚合减少了在路由表中的路由信息量，也减少了交换信息量。RIP-1 不支持子网掩码，如果转发子网路由有可能会引起歧义。所以，RIP-1 始终启用路由聚合功能。如果使用 RIP-2，可以通过 no auto-summary 命令关闭路由聚合功能。当你需要将子网路由广播出去时，可以关闭路由聚合功能。

举例：将 RIP 版本设为 RIP-2 并关闭路由聚合功能。

Switch(Config)#router rip

Switch(Config-Router-Rip(下同))#version 2

Switch(config-router-rip)#no auto-summary

相关命令：**version**

20.3.2.2.2 default-metric

命令：**default-metric <*value*>**

no default-metric

功能：设定引入路由的缺省路由权值；本命令的 no 操作为恢复缺省值。

参数：**<*value*>**为所要设定的路由权值，取值范围 1～16。

缺省情况：缺省的路由权值为 1。

命令模式：RIP 协议配置模式

使用指南：**default-metric** 命令用于设定将其它路由协议的路由引入到 RIP 路由时使用的缺省路由权值。当使用 **redistribute** 命令引入其它协议的路由时，如果不指定具体的路由权值，则以 **default-metric** 所指定的缺省路由权值引入。

举例：设定在 RIP 路由中引入其它路由协议的缺省路由权值为 3。

Switch(config-router-rip)#default-metric 3

相关命令：**redistribute**

20.3.2.2.3 ip rip authentication key-chain

命令：**ip rip authentication key-chain <*name-of-chain*>**

no ip rip authentication key-chain

功能：设置 RIP 验证使用的密钥；本命令 no 操作为取消对 RIP 验证。

参数：**<*name-of-chain*>**字符串，最长不超过 16 个字符。

缺省情况：系统缺省不进行 RIP 验证。

命令模式：接口配置模式

使用指南：本命令的 no 操作为取消 RIP 验证，而不是删除 RIP 验证时使用的密钥。

相关命令：**ip rip authentication**

20.3.2.2.4 ip rip authentication mode

命令：**ip rip authentiaction mode {text|md5**
type {cisco|usual}}
no ip rip authentication mode
功能：设置验证使用的类型；本命令的 no 操作为恢复缺省验证类型即文本验证。
参数：**text** 表示文本验证；**md5** 表示 MD5 验证，并且 MD5 验证又分为 Cisco MD5 和常规 MD5 两种验证方法。
缺省情况：缺省使用文本验证。
命令模式：接口配置模式
使用指南：RIP-I 不支持验证，RIP-II 支持两种验证：文本验证（即 Simple 验证）和数据报验证（即 MD5 验证）。MD5 验证的数据报格式有两种：一种遵循 RFC1723（RIP Version 2 Carrying Additional Information）规定，另一种遵循 RFC2082（RIP-II MD5 Authentication）规定。
举例：在接口 vlan1 上设置 RIP 报文的 Cisoc MD5 验证，验证使用的密钥为 digitalchina。
Switch(config-If-Vlan1)#ip rip authentication mode md5 type cisco
Switch(config-If-Vlan1)#ip rip authentication key-chain digitalchina
相关命令：**ip rip authentication key-chain**

20.3.2.2.5 ip rip metricin

命令：**ip rip metricin <*value*>**
no ip rip metricin
功能：设置在接口接收 RIP 报文增加的附加路由权值；本命令的 no 操作为恢复缺省值。
参数：**<*value*>**为附加的路由权值，取值范围 1～15。
缺省情况：RIP 在接收报文时缺省的附加路由权值为 1。
命令模式：接口配置模式
相关命令：**ip rip metricout**

20.3.2.2.6 ip rip metricout

命令：**ip rip metricout <*value*>**
no ip rip metricout
功能：设置从接口发送 RIP 报文增加的附加路由权值；本命令的 no 操作为恢复缺省值。
参数：**<*value*>**为附加的路由权值，取值范围 0～15。
缺省情况：RIP 在发送报文时缺省的附加路由权值为 0。
命令模式：接口配置模式
举例：在接口 vlan1 接收 RIP 报文附加路由权值 5，发送 RIP 报文附加路由权值 3。
Switch(config-If-Vlan1)#ip rip metricin 5
Switch(config-If-Vlan1)#ip rip metricout 3
相关命令：**ip rip metricin**

20.3.2.2.7 ip rip input

命令：**ip rip input**
no ip rip input

功能：设置接口能够接收 RIP 报文；本命令的
no 操作为接口不能接收 RIP 报文。
缺省情况：接口缺省为接收 RIP 报文。
命令模式：接口配置模式
使用指南：本命令是与其它两条命令 **ip rip output** 和 **ip rip work** 协作使用的，**ip rip work** 从功能上等价于 **ip rip input & ip rip output**，后两条命令分别控制接口上对 RIP 报文的接收和发送，前一项命令等于后两条命令作用之和。
相关命令：**ip rip output**

20.3.2.2.8 ip rip output

命令：**ip rip output**
　　no ip rip output
功能：设置接口能够向外发送 RIP 报文；本命令的 no 操作为接口不能向外发送 RIP 报文。
缺省情况：接口缺省向外发送 RIP 报文。
命令模式：接口配置模式
使用指南：本命令是与其它两条命令 **ip rip output** 和 **ip rip work** 协作使用的，**ip rip work** 从功能上等价于 **ip rip input & ip rip output**，后两条命令分别控制接口上对 RIP 报文的接收和发送，前一项命令等于后两条命令作用之和。
相关命令：**ip rip input**

20.3.2.2.9 ip rip receive version

命令：**ip rip receive version {v1 | v2 | v12}**
　　no ip rip receive version
功能：设置接口接收 RIP 报文的版本信息。缺省接收 RIP 版本 1 和 2；本命令的 no 操作恢复缺省值。
参数：**v1** 和 **v2** 表示 RIP 版本 1 和 RIP 版本 2，**v12** 表示 RIP 版本 1、2。
缺省情况：缺省为 **v12**，即 RIP 版本 1 和 2 全收。
命令模式：接口配置模式

20.3.2.2.10 ip rip send version

命令：**ip rip send version { v1 | v2 [bc|mc] }**
　　no ip rip send version
功能：设置接口发送 RIP 报文的版本；本命令的 no 操作为恢复缺省值。
参数：**v1 | v2** 均为 RIP 的版本号；**[bc|mc]**只在发送 RIP 版本 2 的情况下配置，用于指定发送方式，**BC** 为广播方式，**MC** 为组播方式。当配置发送 RIP 版本 2 报文时，接口缺省以组播 **MC** 方式发送 RIP 版本 2 报文，只有在设置 **BC** 后才能在此接口发送广播报文。
缺省情况：接口缺省发送 RIP 版本 2 报文。
命令模式：接口配置模式
使用指南：当配置接口发送 RIP 版本 2 报文时，缺省发送方式为组播方式，只有设置了 **BC** 方式后才能在此接口发送广播报文。

20.3.2.2.11 ip rip work

命令：**ip rip work**

no ip rip work

功能：设置接口上是否运行 RIP 协议；本命令的 no 操作为本接口不收发 RIP 报文。

缺省情况：打开 RIP 路由开关后，接口上缺省为运行 RIP 协议。

命令模式：接口配置模式

使用指南：本命令在功能上等价于 **ip rip input & ip rip output**，后两条命令分别控制接口上对 RIP 报文的接收和发送，前一项命令等于后两条命令作用之和。

相关命令：**ip rip input**、**ip rip output**

20.3.2.2.12 ip split-horizon

命令：**ip split-horizon**

no ip split-horizon

功能：设置允许水平分割；本命令的 no 操作为禁止水平分割。

缺省情况：缺省情况下，允许水平分割。

命令模式：接口配置模式

使用指南：水平分割用于防止路由循环（Routing Loops），即防止三层交换机把从一个接口上所学习到的路由再从这个接口广播出去。

举例：在接口 vlan1 上设置禁止水平分割。

Switch(config)#interface vlan1

Switch(config-If-Vlan1)#no ip split-horizon

20.3.2.2.13 redistribute

命令：**redistribute { static | ospf | bgp} [metric <*value*>]**

no redistribute { static | ospf | bgp }

功能：在 RIP 路由中引入其它路由协议的路由；本命令的 no 操作为取消引入。

参数：**static** 指定引入静态路由；**ospf** 指定引入 OSPF 路由；**bgp** 指定引入 BGP 路由；**<*value*>**指定以多大的路由权值引入路由，取值范围 1～16。

缺省情况：RIP 缺省不引入其它路由。如果引入其它的路由协议而不指定它的 metric 值，则按缺省路由权值 **default-metric** 引入。

命令模式：RIP 配置模式

使用指南：采用本命令可以引入其他的路由作为 RIP 自己的路由，提高 RIP 的性能。

举例：在 RIP 报文中引入 OSPF 协议路由的路由权值为 5，静态路由的路由权值为 8。

Switch(Config-Router-Rip)#redistribute ospf metric 5

Switch(Config-Router-Rip)#redistribute static metric 8

20.3.2.2.14 rip broadcast

命令：**rip broadcast**

no rip broadcast

功能：配置三层交换机的的所有接口发 RIP 广播包或组播包；本命令的 no 操作禁止各端口发广播包或组播包，而只能在配置了 neighbor 的三层交换机之间发送 RIP 数据包。
缺省情况：系统缺省发 RIP 广播包。
命令模式：RIP 配置模式

20.3.2.2.15 rip checkzero

命令：rip checkzero
no rip checkzero
功能：使用本命令对 RIP-1 报文的零域进行检查；本命令的 no 操作为取消对零域的查零操作。由于 RIP-2 的报文中没有零域，所以本命令对 RIP-2 没有作用。
缺省情况：系统缺省对 RIP-1 报文进行查零操作。
命令模式：RIP 协议配置模式
使用指南：在 RIP-1 的报文中必须有零域（zero field），可以使用本命令来启动和禁止对 RIP-1 报文的查零操作。如果进行查零操作时，若收到零域不为零的 RIP-1 报文，系统将丢弃该 RIP-1 的报文。
举例：设置不再对 RIP-1 报文进行查零操作。
Switch(config-router-rip)#no ip checkzero

20.3.2.2.16 rip preference

命令：rip preference <*value*>
no rip preference
功能：指定 RIP 协议的路由优先级；本命令的 no 操作为恢复缺省值。
参数：<*value*> 指定优先级的值，取值范围为 0～255。
缺省情况：系统缺省指定 RIP 的优先级是 120。
命令模式：RIP 协议配置模式
使用指南：每一种路由协议都有自己的优先级，它的缺省取值由具体的路由策略决定。优先级的高低将决定在核心路由表中的路由采取哪种路由算法获取的最佳路由。可以利用本命令手动调整 RIP 的优先级，优先级调整后，对新路由生效。由 RIP 协议的性质决定，RIP 的优先级不宜过高。
举例：设置 RIP 的优先级为 10。
Switch(config-router-rip)#rip prefenrence 10

20.3.2.2.17 router rip

命令：router rip
no router rip
功能：启动 RIP 路由协议并进入 RIP 配置模式；本命令的 no 操作为关闭 RIP 路由协议。
缺省情况：不运行 RIP 路由。
命令模式：全局配置模式
使用指南：本命令是 RIP 路由协议的启动开关，进行 RIP 协议的其他配置要先打开本命令。
举例：启动 RIP 协议配置模式。

Switch(Config)#router rip
Switch(Config-Router-Rip)#

20.3.2.2.18 timer basic

命令：timer basic <*update*> <*invalid*> <*holddown*>
no timer basic
功能：调整 RIP 计时器更新、期满、抑制的时间；本命令的 no 操作为恢复各项参数的缺省值。
参数：*<update>*发送更新报文的时间间隔，单位秒，取值范围 1～2147483647；***<invalid>***宣布 RIP 路由无效的时间段，单位秒，取值范围 1～2147483647；***<holddown>***为宣布某路由无效后仍可在路由表中存在的时间段，单位秒，取值范围 1～2147483647。
缺省情况：*<update>*缺省值 30；***<invalid>***缺省值 180；***<holddown>***缺省值 120。
命令模式：RIP 协议配置模式
使用指南：缺省情况下，系统每 30 秒会广播 RIP 更新报文；当过了 180 秒不能收到某路由的更新报文，就认为该路由无效；但该路由还能在路由表中存在 120 秒，120 秒后，在路由表删除该路由。在调整 RIP 各项计时器时间时要注意，宣布 RIP 路由无效时间至少应大于 RIP 更新的时间，holddown 的时间段（即宣布 RIP 路由无效后，在路由表中删除该项路由的时间）也至少应该大于 RIP 更新的时间，且必须为整数倍。
举例：设置 RIP 路由表更新时间为 20 秒，宣布无效时间为 80 秒，删除路由项的时间为 60 秒。
Switch(Config-Router-Rip)#timer basic 20 80 60

20.3.2.2.19 version

命令：version {1| 2}
no version
功能：设置所有路由器接口发送/接收 RIP 数据报的版本；no 操作恢复缺省设置
参数：1 为 rip 版本 1；**2** 为 rip 版本 2。
缺省情况：发送版本 1，接收版本 1 和 2 的数据报。
命令模式：RIP 协议配置模式
使用指南：1 表示三层交换机各接口只发送/接收 RIP-I 数据报，2 表示三层交换机各接口只发送/接收 RIP-II 数据报。缺省情况下，发送 RIP-II 同时接收 RIP-I 和 RIP-II 数据报。
举例：设置该交换机接口发送/接收 RIP 数据报的版本为 2。
Switch(config-router-rip)#version 2
相关命令：ip rip receive version
ip rip send version

20.3.2.2.20 show ip protocols

命令：show ip protocols
功能：显示三层交换机当前运行的路由协议的信息。

命令模式：特权用户配置模式

使用指南：根据本命令的输出信息，用户可以确认配置的路由协议是否正确和进行路由故障诊断。

举例：

Switch#sh ip protocols
RIP information
rip is turning on
default metrict 16
neighbour is:NULL
preference is 100
rip version information is:

interface	send version	receive version
vlan2	V2BC	V12
vlan3	V2BC	V12
vlan4	**V2BC**	**V12**

显示信息	解释
RIP is turning on	正在运行的路由协议为 RIP 协议；
default metric	RIP 协议缺省度量值；
neighbour is:	与本 RIP 三层交换机相连的邻居三层交换机 IP 地址
Preference	RIP 路由的优先级；
rip version information	显示运行 RIP 协议的版本信息，包括发送 RIP 版本（V1 表示 RIP-1，V2 表示 RIP-2），RIP 发送方式（BC 表示广播，MC 表示组播），接收 RIP 版本（V1 表示 RIP-1，V2 表示 RIP-2，V12 表示同时接收 RIP-1 和 RIP-2）。

20.3.2.2.21 show ip rip

命令：show ip rip

功能：显示 RIP 当前运行状态及配置信息。

命令模式：特权用户配置模式

使用指南：根据本命令的输出信息，用户可以查看 RIP 路由的缺省权值、指定发送的目标地址、优先值等。

举例：

Switch#sh ip rip
RIP information
rip is turning on
default metric 16
neighbour is
preference is 100

显示信息	解释
rip is turning on	RIP 路由进程已打开；
default metric 16	默认引入路由的权值为 16；

neighbour is	定点发送的目标地址；
preference is 100	RIP 路由的优先级为 100。

20.3.2.2.22 debug ip rip packet

命令：**debug ip rip packet**

no debug ip rip packet

功能：打开 RIP 报文的收发信息调试开关；本命令的 no 操作为关闭调试开关。

缺省情况：调试开关关闭。

命令模式：特权用户配置模式

举例：

```
Switch#debug ip rip pa
"debug ip rip pa" executed successfully.
00：04：20：

start at 260*********************
send packets to           11.11.11.2
packet header:     cmd:   response, version:   1
no.         dest                 dest_mask         gatedway   metric
1:          159.226.0.0            0.0.0.0            0.0.0.0    1
00：04：20：

start at 260*********************
send packets to    159.226.255.255
packet header:     cmd:   response, version:   1
no.         dest                dest_mask          gatedway   metric
1:          159.222.0.0         0.0.0.0            0.0.0.0       2
2:          11.11.11.2          0.0.0.0            0.0.0.0       2
00：04：20：

start at 260*********************
received a rip packet from           159.226.42.1
rip packet cmd  :  2     version:  1
```

20.3.2.2.23 debug ip rip recv

命令：**debug ip rip recv**

no debug ip rip recv

功能：打开 RIP 报文的接收信息的调试开关；本命令的 no 操作为关闭调试开关。

缺省情况：调试开关关闭。

命令模式：特权用户配置模式

举例：

Switch#debug ip rip rec

start at 230*********************
received a rip packet from 159.226.42.1
rip packet cmd ： 2 version：1
00：03：59：

start at 238*********************
received a rip packet from 11.11.11.2
rip packet cmd ： 2 version：1
00：03：59：
rip receive response
packet head 14872964; packet end 14872984
recv packets from 11.11.11.2
packet header： cmd： response, version： 1

no.	dest	dest_mask	gatedway	metric
1：	159.222.0.0	0.0.0.0	0.0.0.0	1

20.3.2.2.24 debug ip rip send

命令：**debug ip rip send**

no debug ip rip send

功能：打开 RIP 报文的发送信息的调试开关；本命令的 no 操作为关闭调试开关。

缺省情况：调试开关关闭。

命令模式：特权用户配置模式

举例：

Switch#debug ip rip send
00：02：50：
start at 170*********************
send packets to 11.11.11.2
packet header： cmd： response, version： 1

no.	dest	dest_mask	gatedway	metric
1：	159.226.0.0	0.0.0.0	0.0.0.0	1

00：02：50：

start at 170*********************
send packets to 159.226.255.255
packet header： cmd： response, version： 1

no.	dest	dest_mask	gatedway	metric
1：	159.222.0.0	0.0.0.0	0.0.0.0	2
2：	11.11.11.2	0.0.0.0	0.0.0.0	2

20.3.3 RIP 典型案例

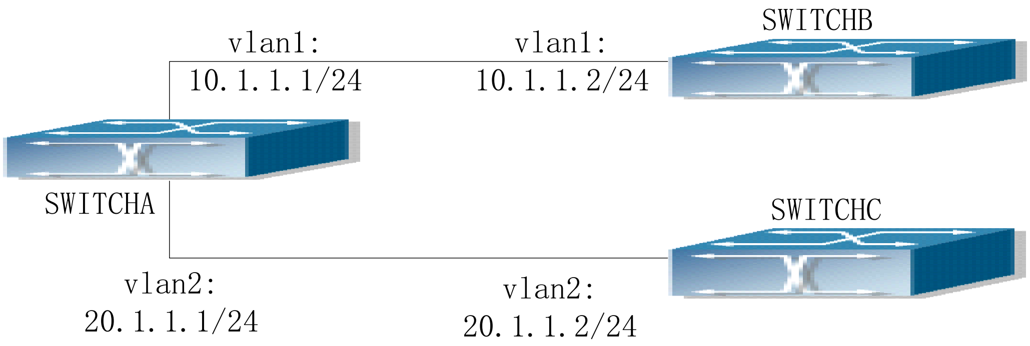


图 20-2 RIP 案例

图为三台三层交换机组成的一个网络，三层交换机 SWITCHA 与三层交换机 SWITCHB 和三层交换机 SWITCHC 分别通过接口 vlan1 和接口 vlan2 相连，三台三层交换机都运行 RIP 路由协议。设三层交换机 SWITCHA vlan1：10.1.1.1， vlan2：20.1.1.1 只与三层交换机 SWITCHB vlan1：10.1.1.2 交流三层交换机更新信息，而不向三层交换机 SWITCHC vlan2：20.1.1.2 交流三层交换机更新信息。

三层交换机 SWITCHA、SWITCHB、SWITCHC 的配置分别如下：

a) 三层交换机 SWITCHA：

!配置接口 vlan1 的 IP 地址。
SWITCHA#config
SWITCHA(config)# interface vlan 1
SWITCHA(Config-If-Vlan1)# ip address 10.1.1.1 255.255.255.0
SWITCHA (config-If-vlan1)#exit
!配置接口 vlan2 的 IP 地址
SWITCHA(config)# interface vlan 2
SWITCHA(config-If-vlan2)# ip address 20.1.1.1 255.255.255.0
！ 启动 RIP 协议
SWITCHA(config)#router rip
SWITCHA(config-router-rip)#exit
！ 使能接口 vlan1 发送/接收 RIP 数据报
SWITCHA(config)#interface vlan 1
SWITCHA(config-If-vlan1)#ip rip work
SWITCHA(config-If-vlan1)#exit
！ 使能接口 vlan2 发送/接收 RIP 数据报
SWITCHA (config-If-vlan2)# ip rip work
SWITCHA (config-If-vlan2)#exit
SWITCHA(config)#exit
SWITCHA#

b) 三层交换机 SWITCHB：

!配置接口 vlan1 的 IP 地址。
SWITCHB#config
SWITCHB(config)# interface vlan 1

SWITCHB(config-If-vlan1)# ip address 10.1.1.2 255.255.255.0
SWITCHB (config-If-vlan1)exit
！启动 RIP 协议，配置邻居三层交换机 IP 地址
SWITCHB(config)#router rip
SWITCHB(config-router-rip)#exit
！使能接口 vlan1 发送/接收 RIP 数据报
SWITCHB(config)#interface vlan 1
SWITCHB (config-If-vlan1)#ip rip work
SWITCHB (config-If-vlan1)#exit
SWITCHB(config)#exit
SWITCHB#

c) 三层交换机 SWITCHC：
!配置接口 vlan2 的 IP 地址。
SWITCHC#config
SWITCHC(config)# interface vlan 2
SWITCHC(config-If-vlan2)# ip address 20.1.1.2 255.255.255.0
SWITCHC (c config-If-vlan2)#exit
！启动 RIP 协议
SWITCHC(config)#router rip
SWITCHC(config-router-rip)#exit
！使能接口 vlan2 发送/接收 RIP 数据报
SWITCHC(config)#interface vlan 2
SWITCHC (config-If-vlan2)#ip rip work
SWITCHC (config-If-vlan2)exit
SWITCHC(config)#exit
SWITCHC#

20.3.4 RIP 排错帮助

1.监测和调试命令
2.RIP 排错帮助

20.3.4.1 监测和调试命令

命令	解释
特权模式	
show ip rip	显示 RIP 当前运行状态及配置信息。根据该命令的输出信息，用户可以确认配置是否正确和进行 RIP 故障诊断。
show ip route	显示路由表信息，可以查看有关 RIP 路由信息
show ip protocols	显示协议信息。
[no] debug ip rip packet	显示收发的所有 RIP 数据报。

[no] debug ip rip recv	显示收到的所有 RIP 数据报。
[no] debug ip rip send	显示发出的所有 RIP 数据报。

（1）show ip rip

显示信息为：

RIP information:

Automatic network summarization is not in effect.

default metric for redistribute is :16

neigbour is :NULL

preference is :100

显示信息说明：

显示信息	解释
Automatic network summarization is not in effect	RIP 自动聚合功能关闭；
default metric for redistribute is :16	默认引入路由的权值为 16；
neigbour is	定点发送的目标地址；
preference is :100	RIP 路由的优先级为 100。

（2）show ip route

使用 show ip route 命令可以显示路由表中关于 RIP 路由的目的 IP 地址、网络掩码以及下一跳 IP 地址或转发接口等信息。

例如，显示信息为：

```
Switch#show ip route
Total route items is 2, the matched route items is 2
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived, D - DVMRP derived

   Destination    Mask            Nexthop      Interface    Pref
C  2.2.2.0        255.255.255.0   0.0.0.0      vlan1        0
R  7.7.7.0        255.255.255.0   2.2.2.8      vlan2        100
```

其中，R 表示 RIP 路由，即目的网络地址为 7.7.7.0、网络掩码为 255.255.255.0、下一跳地址为 2.2.2.8 以及转发接口为以太网口 vlan2 的一条路由为 RIP 路由，它的优先级为 100。

（3）show ip protocols

使用 show ip protocols 命令可以显示当前三层交换机运行路由协议的信息。

例如，显示信息为：

```
Switch#sh ip protocols
RIP information:
Automatic network summarization is not in effect.
default metric for redistribute is :16
neigbour is:NULL
preference is :100
RIP version information is:
interface      send version      receive version
vlan1            V2BC                V12
vlan2            V2BC                V12
```

vlan3 V2BC
V12
Switch#

显示信息	解释
Automatic network summarization is not in effect	RIP 自动聚合功能关闭;
default metric for redistribute is :	RIP 协议缺省度量值;
neigbour is:	与本 RIP 三层交换机相连的邻居三层交换机 IP 地址
Preference	OSPF 路由的优先级;
RIP version information	显示运行 RIP 协议的版本信息，包括发送 RIP 版本（V1 表示 RIP-I，V2 表示 RIP-II），RIP 发送方式（BC 表示广播，MC 表示组播），接收 RIP 版本（V1 表示 RIP-I，V2 表示 RIP-II，V12 表示同时接收 RIP-I 和 RIP-II）。

20.3.4.2 RIP 排错帮助

在配置、使用 RIP 协议时，可能会由于物理连接、配置错误等原因导致 RIP 协议未能正常运行。因此，用户应注意以下要点：

- ✧ 首先应该保证物理连接的正确无误；
- ✧ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ✧ 然后，先启动 RIP 协议（使用 router rip 命令）再在相应接口配置 RIP 协议参数，如使用的是 RIP-I 还是 RIP-II 等；
- ✧ 接着，注意 RIP 协议的自身特点——RIP 三层交换机每隔 30 秒向它所有邻居三层交换机发送路由表更新信息，如果 180 秒内没有收到来自某三层交换机的信息，那么认为该三层交换机崩溃或相连的网络不可达，到该三层交换机的路由还将在路由表中保持 120 秒然后被删除。因此，如果删除某个 RIP 路由，需等待 300 秒后才能保证路由表中除去此路由项。

如果仍无法解决 RIP 路由问题，那么请使用 debug ip rip 调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给神州数码技术服务中心。

20.4 OSPF

20.4.1 OSPF 介绍

OSPF（Open Shortest Path First）协议即"开放最短路径优先协议"。它是一种基于链路状态的自治系统内部的动态路由协议，它通过三层交换机间交换链路状态信息来组成一个链路状态数据库，然后基于这个数据库用最短路径优先算法生成路由表。

自治系统（AS）是一个自我管理的互连网络。在大型网络中，例如Internet，极大的互连网络被分解为自治系统。连接到Internet上的大型公司网络是独立的自治系统，因为Internet上的其他主机并不由它来管理，而且它和Internet三层交换机并不共享内部路由选择

信息。

每个链路状态三层交换机可提供与其邻居三层交换机的拓扑结构的信息：

- 三层交换机所连接的网段（链路）
- 连接链路的状态

链路状态信息在网络上泛洪（flooding），目的是使所有的三层交换机可以接收到第一手信息。链路状态三层交换机并不会广播包含在它们的路由表内的所有信息，相反链路状态三层交换机将发送关于已经改动的链路状态信息。链路状态三层交换机将向它们的邻居发送呼叫信息建立邻接关系，然后在邻接三层交换机之间发送链路状态通告（LSA）。邻接三层交换机将LSA复制到它们的路由选择表中，并传递这些信息到网络的剩余部分。这个过程称为泛洪（flooding）。这样，实现了向网络发送第一手信息，为网络建立更新路由的准确映射。链路状态路由选择协议使用称为代价的方法（而不是使用跳）来选择路径。代价是自动或人工赋值的。根据链路状态协议的算法，代价可以计算数据包必须穿越的跳数目、链路带宽、链路上的当前负载，甚至可以由管理员加入的权重来评价。

1) 当一个链路状态三层交换机进入链路状态互连网络时，它发送一个呼叫数据包（HELLO）以了解其邻居，并建立邻接关系。

2) 邻居用关于它们所连接的链路以及相关的代价度的信息进行应答。

3) 起始的三层交换机用这个信息来建立它的路由选择表。

4) 然后，作为定期更新的一部分。三层交换机向它的邻接三层交换机发送链路状态数据包。这个LSA包括了那个三层交换机的链路及相关代价。

5) 每个邻接三层交换机复制该LSA数据包，并且将LSA传递到下一个邻居（即泛洪）。

6) 因为三层交换机并没有在向前泛洪LSA之前重新计算路由选择数据库，因此收敛时间大大减少了。

链路状态路由选择协议的一个主要优点就是这样的一个事实，即路由无穷记数不可能形成，原因是链路状态协议独立建立它们自己的路由选择信息表的方式。第二个优点是，在链路状态互连网络中收敛是非常快的，原因是一旦路由选择拓扑出现变动，则更新在互连网络上迅速泛洪。这些优点又释放了三层交换机的资源，因为对不好的路由信息所花费的处理能力和带宽消耗都很少。

OSPF协议的特点：OSPF协议支持各种规模的网络，最多可以支持几百台三层交换机；路由拓扑结构变化后OSPF能够立即发送链路状态更新数据包，收敛迅速；OSPF根据收集到的链路状态采用最短路径算法计算路由，保证了无自环路由；OSPF将自治系统划分为多个域，减小了数据库尺寸、减少了占用网络带宽、降低了计算负担（根据三层交换机在自治系统中所处的位置可以划分为域内三层交换机、域边界三层交换机、自治系统边界三层交换机和骨干三层交换机）；OSPF支持负载分担，支持到同一目的地址的多条等价路由；OSPF支持4级路由机制（按域内路由、域间路由、第一类外部路由和第二类外部路由顺序分级处理路由）；OSPF协议支持IP子网、支持与其他路由协议的路由的引入、支持基于接口的报文验证；OSPF支持组播发送数据包。

每个OSPF三层交换机都维护着一份描述整个自治系统拓扑结构的数据库。每一台三层交换机都搜集本地状态的信息，如可用接口信息，可达邻居信息，然后通过使用链路状态通告（即向外发送链路状态信息），本三层交换机与其他OSPF三层交换机交换链路状态信息，从而形成描述整个自治系统的链路状态数据库。根据链路状态数据库，各三层交换机构建一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由。如果存在两台或两台以上的三层交换机（即多路访问网络），该网络上要选出"指定三层交换机"和"备份指定三层交换机"，指定三层交换机负责将网络的链路状态播出去，引入这一概念，有助于减少在多路访问网络上各三层交换机之间的数据流量。

OSPF协议要求将自治系统的网络划分
成区域来管理，即将自治系统划分为0域（骨干域）和非0域，区域间传送的路由信息被进一步抽象概括，从而减少了整个网络的实用带宽。OSPF使用4类不同的路由，按优先顺序来说分别是区域内路由、区域间路由、第一类外部路由和第二类外部路由。区域内和区域间路由描述的是自治系统内部的网络结构，而外部路由则描述了应该如何选择到自治系统以外的目的地。第一类外部路由对应于OSPF从其它内部路由协议所引入的信息，这些路由的开销和OSPF自身路由的开销具有可比性；第二类外部路由对应于OSPF从外部路由协议所引入的信息，它们的开销远大于OSPF自身的路由开销，所以在计算路由开销时，不考虑OSPF自身的路由开销。

OSPF的区域以Backbone（骨干区域）作为核心，该区域标识为0域，所有的其他区域都必须与0域在逻辑上相连，0域必须保证连续。为此，骨干区域上特别引入了虚连接的概念以保证即使在物理上分割的该区域仍然在逻辑上具有连通性。在同一区域内的所有三层交换机的配置要保持一致。

如上所述，LSA只能在邻接三层交换机之间进行传递，OSPF协议包括五类LSA：路由器LSA、网络LSA、到其它域所在网络的汇总LSA、到自治系统边界三层交换机的汇总LSA和自治系统外部LSA。它们也可分别叫做类型1LSA、类型2LSA、类型3LSA、类型4LSA和类型5LSA。路由器LSA由OSPF域内的每个三层交换机产生，并发送给域内所有其它邻接三层交换机；网络LSA是由多路访问网络所在OSPF域的指定三层交换机产生的（为减少多路访问网络上各三层交换机之间的数据流量，多路访问网络中需要选出“指定三层交换机”和“备份指定三层交换机”，由指定三层交换机负责将网络的链路状态播出去），并发送给域内所有其它邻接三层交换机；汇总LSA由OSPF域边界三层交换机产生，并在域边界三层交换机之间传送；自治系统外部LSA由自治系统外部边界三层交换机产生，并在整个自治系统内传递。

对于以外部链路状态通告为主的自治系统，为减少拓扑数据库的尺寸，OSPF允许将某些域配置成STUB域。类型4LSA（ASBR汇总LSA）和类型5LSA（AS外部LSA）等两种LSA不允许泛滥进入/通过STUB域。STUB域内必须使用缺省路由，STUB域的域边界三层交换机通过汇总类型3LSA来通告到STUB域的缺省路由；这些缺省路由只在STUB内泛滥，不泛滥到STUB域之外。每个STUB域对应一条缺省路由，STUB域到AS外部目的地的路由只依赖该域的缺省路由。

OSPF协议路由的简单计算过程如下：

1） 每个支持 OSPF 协议的三层交换机都维护着一个描述整个自治系统拓扑结构的链路状态数据库（即 LS 数据库）。每个三层交换机根据自己周围的网络拓扑结构生成一条链路状态通告（即路由器 LSA），通过相互之间发送链路状态更新包（LSU）将各自的 LSA 发送给网络中的其它三层交换机。这样，每台三层交换机都收到了其它三层交换机的 LSA，所有 LSA 在一起便形成了链路状态数据库。
2） 由于一条 LSA 是对该三层交换机周围网络拓扑结构的描述，那么 LS 数据库则是对整个网络的拓扑结构的描述。三层交换机很容易根据 LS 数据库建立一张带权有向图，显然自治系统内的所有三层交换机都将得到一张相同的网络拓扑图。
3） 每台三层交换机都使用最短路径 SPF 算法计算出一棵以自己为根的最短路径树，该树给出了到自治系统中各个节点的路由，外部路由信息为叶子节点，外部路由可根据广播它的三层交换机进行标记以记录关于自治系统的额外信息。由此可见，各个三层交换机得到的路由表是不同的。

OSPF 协议是 IETF 组织开发的，目前广泛使用的是 OSPFv2 版本是参照 RFC2328 中描述的内容实现的。

20.4.2 OSPF 配置

DCRS 系列三层交换机的 OSPF 配置有自身的特点，简单说分两步：1、在全局使能 OSPF；2、在接口配置 OSPF 域。这与其它厂商会配置方法有不同。

20.4.2.1 配置任务序列

1. 启动 OSPF 协议（必须）
   （1）启动/关闭 OSPF 协议（必须）
   （2）配置运行 OSPF 三层交换机的 ID 号（可选）
   （3）配置运行 OSPF 的网络范围（可选）
   （4）配置接口所属的域（必须）
2. 配置 OSPF 辅助参数（可选）
   （1）配置 OSPF 发包机制参数
      1）配置 OSPF 数据包的验证
      2）配置 OSPF 接口为只收不发
      3）配置接口发送数据包的代价
      4）配置 OSPF 发包定时器参数（广播接口轮询发送 HELLO 数据包的定时器、邻接三层交换机失效定时器、接口传送 LSA 时延定时器、邻接三层交换机重传 LSA 定时器）
   （2）配置 OSPF 引入路由参数
      1）配置引入外部路由的缺省参数（缺省类型、缺省标记值、缺省代价值、缺省时间间隔和缺省数量上限）
      2）配置在 OSPF 中引入其它协议的路由
   （3）配置 OSPF 协议其它参数
      1）配置 OSPF 路由协议优先级
      2）配置 OSPF STUB 域及缺省路由的代价
      3）配置 OSPF 虚链路
      4）配置接口在选举指定三层交换机 DR 中的优先级
3. 关闭 OSPF 协议

1. 启动 OSPF 协议

在 DCRS 系列三层交换机上运行 OSPF 路由协议的基本配置也很简单，通常只需打开 OSPF 开关、配置接口所在 OSPF 域即可，OSPF 协议的参数都使用缺省值。如需修改 OSPF 协议参数值，参看 2.配置 OSPF 辅助参数。

命令	解释
全局配置模式	
[no] router ospf	启动 OSPF 协议，本命令的 no 操作关闭 OSPF 协议。（必须）
router id <*router_id*> **no router id**	配置运行 OSPF 协议三层交换机的 ID 号；本命令的 no 操作取消三层交换机的 ID 号。缺省为选择某个接口的 IP 地址作为三层交换机 ID。（可选）

OSPF 协议配置模式	
[no] network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]	将一个区域中几个网段定义成一个网络范围，本命令的 no 命令取消网络范围。（可选）
接口配置模式	
ip ospf enable area <*area_id*> **no ip ospf enable area**	配置某个接口属于某个区域，本命令的 no 操作为取消该配置。（必须）

2. 配置 OSPF 辅助参数

（1）配置 OSPF 发包机制参数

1）配置 OSPF 数据包的验证

2）配置 OSPF 接口为只收不发

3）配置接口发送数据包的代价

命令	解释
接口配置模式	
ip ospf authentication { simple <*auth_key*>| md5 <*auth_key*> <*key_id*>} **no ip ospf authentication**	配置接口接受 OSPF 数据包所需要的验证方式及验证密钥；本命令的 no 操作恢复为缺省值。
[no] ip ospf passive-interface	将一个接口设置为只收不发；本命令的 no 操作取消配置。
ip ospf cost <*cost* > **no ip ospf cost**	指定接口运行 OSPF 协议所需的代价；本命令的 no 操作恢复代价的缺省值。

4）配置 OSPF 发包定时器参数（广播接口轮询发送 HELLO 数据包的定时器、邻接三层交换机失效定时器、接口传送 LSA 时延定时器、邻接三层交换机重传 LSA 定时器）

命令	解释
接口配置模式	
ip ospf hello-interval <*time*> **no ip ospf hello-interval**	配置接口周期发送 HELLO 数据包的时间间隔；本命令的 no 操作恢复为缺省值。
	该行删去
ip ospf dead-interval <*time* > **no ip ospf dead-interval**	配置认定相邻三层交换机失效的时间间隔；本命令的 no 操作恢复为缺省值。
ip ospf transmit-delay <*time*> **no ip ospf transmit-delay**	设置在接口上传送链路状态广播的时延值；本命令的 no 操作恢复为缺省值。
ip ospf retransmit <*time*> **no ip ospf retransmit**	配置接口与邻接三层交换机之间传送链路状态通告时的重传间隔；本命令的 no 操作恢复为缺省值。

（2）配置 OSPF 引入路由参数

1）配置引入外部路由的缺省参数（缺省类型、缺省标记值、缺省代价值、缺省时间间隔和缺省数量上限）

命令	解释

OSPF 协议配置模式	
default redistribute type { 1 | 2 } **no default redistribute type**	配置引入外部路由时缺省的类型；本命令的 no 操作恢复缺省值。
default redistribute tag <*tag*> **no default redistribute tag**	配置引入外部路由时缺省的标记值；本命令的 no 操作取消标记值。
default redistribute cost <*cost*> **no default redistribute cost**	配置引入外部路由时缺省的代价值；本命令的 no 操作取消引入外部路由时的缺省代价值。
default redistribute interval <*time*> **no default redistribute interval**	配置 OSPF 引入外部路由的时间间隔；本命令的 no 操作恢复缺省值。
default redistribute limit <*routes*> **no default redistribute limit**	配置 OSPF 可引入路由数量的上限；本命令的 no 操作恢复缺省值。

2）配置在 OSPF 中引入其它协议的路由

命令	解释
OSPF 协议配置模式	
redistribute ospfase { bgp | connected | static | rip} [type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>] **no redistribute ospfase { bgp | connected | static | rip }**	引入 BGP 路由、直连路由、静态路由和 RIP 路由作为外部路由信息；本命令的 no 操作取消引入的外部路由信息。

（3）配置 OSPF 协议其它参数

1）配置 OSPF 路由协议优先级

2）配置 OSPF STUB 域及缺省路由的代价

3）配置 OSPF 虚链路

命令	解释
OSPF 协议配置模式	
preference [ase] <*preference* > **no preference [ase]**	配置 OSPF 协议在各路由协议之间的优先级，以及引入的自治系统外部路由的优先级；本命令的 no 操作恢复缺省值。
stub cost <*cost*> area <*area_id* > **no stub area <area_id >**	将一个区域定义成 stub 区域；本命令的 no 操作取消 STUB 域。
virtuallink neighborid <*router_id*> transitarea <*area_id*> [hellointerval <*time*>] [deadinterval <*time*>] [retransmit <*time*>] [transitdelay <*time*>] **no virtuallink neighborid <*router_id*> transitarea <*area_id*>**	创建并配置虚连接；本命令的 no 操作删除一条虚链接。

4）配置接口在选举指定三层交换机 DR 中的优先级

命令	解释
接口配置模式	

ip ospf priority <*priority*> no ip ospf priority	配置接口在选举"指定三层交换机"时的优先级；本命令的 no 操作为恢复优先级缺省值。

3. 关闭 OSPF 协议

命令	解释
全局配置模式	
no router ospf	关闭 OSPF 路由协议。

20.4.2.2 OSPF 的配置命令

- **default redistribute cost**
- **default redistribute interval**
- **default redistribute limit**
- **default redistribute tag**
- **default redistribute type**
- **ip opsf authentication**
- **ip ospf cost**
- **ip opsf dead-interval**
- **ip ospf enable area**
- **ip ospf hello-interval**
- **ip ospf passive-interface**
- **ip ospf priority**
- **ip ospf retransmit-interval**
- **ip ospf transmit-delay**
- **network**
- **preference**
- **redistribute ospfase**
- **router id**
- **router ospf**
- **stub cost**
- **virtuallink neighborid**
- **show ip ospf**
- **show ip ospfase**
- **show ip ospf cumulative**
- **show ip ospf database**
- **show ip ospf interface**
- **show ip ospf neighbor**
- **show ip ospf routing**
- **show ip ospf virtual-links**
- **show ip protocols**
- **debug ip ospf event**
- **debug ip ospf lsa**
- **debug ip ospf packet**

- **debug ip ospf spf**

20.4.2.2.1 default redistribute cost

命令：default redistribute cost <*cost*>

no default redistribute cost

功能：配置 OSPF 引入外部路由时缺省的花费值；本命令的 no 操作为恢复缺省值。

参数：<*cost*>为花费值，取值范围 1～65535。

缺省情况：缺省设置引入的花费值为 1。

命令模式：OSPF 协议配置模式

使用指南：OSPF 路由协议引入由其它路由协议发现的路由时，把这些路由信息作为自己的自治系统外部的路由信息。引入外部路由信息需要一些额外的参数，如：路由的缺省花费和缺省的标记等。本命令提供给用户可据实际情况设置合理的引入外部路由时缺省花费值。

举例：设置 OSPF 引入外部路由的缺省花费值为 20。

Switch(Config-Router-Ospf)#default redistribute cost 20

20.4.2.2.2 default redistribute interval

命令：default redistribute interval <*time*>

no default redistribute interval

功能：配置 OSPF 引入外部路由的时间间隔；本命令的 no 操作为恢复缺省值。

参数：<*time*>为引入外部路由的时间间隔，单位为秒，取值范围 1～65535。

缺省情况：OSPF 引入外部路由的时间间隔缺省为 1 秒。

命令模式：OSPF 协议配置模式

使用指南：OSPF 会定期的引入外部的路由信息，并将这些路由信息传播到整个自治系统中，本命令用于修改引入外部路由信息的时间间隔。

举例：OSPF 引入外部路由的时间间隔为 3 秒。

Switch(Config-Router-Ospf)#default redistribute interval 3

20.4.2.2.3 default redistribute limit

命令：default redistribute limit <*routes*>

no default redistribute limit

功能：配置 OSPF 一次可引入外部路由的最大值；本命令的 no 操作为恢复缺省值。

参数：<*routes*>为引入路由数量的最大值，取值范围 1～65535。

缺省情况：OSPF 引入外部路由数量的最大值缺省为 100。

命令模式：OSPF 协议配置模式

使用指南：OSPF 定期引入外部的路由信息并将它们传播到整个自治系统中，本命令规定在一次能够引入的外部路由信息的最大条数。

举例：设置 OSPF 一次最多可引入 110 条外部路由。

Switch(Config-Router-Ospf)#default redistribute limit 110

20.4.2.2.4 default redistribute tag

命令：**default redistribute tag <*tag*>**

no default redistribute tag

功能：配置引入外部路由时缺省的标记值；本命令的 no 操作为恢复缺省值。

参数：**<*tag*>**为标记值，取值范围 0～4294967295。

缺省情况：缺省值为 0。

命令模式：OSPF 协议配置模式

使用指南：OSPF 路由协议引入由其它路由协议发现的路由时，把这些路由信息作为自己的自治系统外部的路由信息。引入外部路由信息需要一些额外的参数，如：路由的缺省花费和缺省的标记等。本命令为用户提供路由标记标识协议相关的信息。

举例：设置 OSPF 引入外部路由时缺省的标记值为 20000

Switch(Config-Router-Ospf)#default redistribute tag 20000

20.4.2.2.5 default redistribute type

命令：**default redistribute type { 1 | 2 }**

no default redistribute type

功能：配置引入外部路由时缺省的类型；本命令的 no 操作为恢复缺省值。

参数：**1 | 2** 分别表示第一类外部路由和第二类外部路由。

缺省情况：系统缺省认为引入的外部路由为第二类外部路由。

命令模式：OSPF 协议配置模式

使用指南：OSPF 在协议中规定了两类外部路由信息的代价选择方式：第一类外部路由和第二类外部路由。第一类外部路由的代价=外部路由的通告代价+从某个三层交换机到通告三层交换机（AS 外部三层交换机）的代价。第二类外部路由的代价=外部路由的通告代价。第一类和第二类外部路由同时存在的时，第一类外部路由代价的优先级高。

举例：设置 OSPF 引入外部路由时缺省的类型为 type 1

Switch(Config-Router-Ospf)#default redistribute type 1

20.4.2.2.6 ip ospf authentication

命令：**ip ospf authentication { simple <*auth_key*>| md5 <*auth_key*> <*key_id*>}**

no ip ospf authentication

功能：指定接口上接受 OSPF 报文所需要的验证方式；本命令的 no 操作为取消验证。

参数：**simple** 为简单验证方式；**md5** 为 MD5 加密验证方式；**<*auth_key*>** 验证密钥，为连续的字符串，简单验证方式下最大长度为 8 字节，MD5 验证方式下最大长度为 16 字节；**<*key_id*>**为 MD5 验证方式时的验证字，取值范围 1～255。

缺省情况：接口上接受 OSPF 报文缺省不需要验证。

命令模式：接口配置模式

使用指南：密钥的值将写入 OSPF 报文中，为保证三层交换机与相邻三层交换机之间 OSPF 报文的正常收发，必须在对端设置相同的密钥参数。

举例：在 OSPF 接口 vlan1 配置 MD5 验证方式，验证密码为 123abc。

Switch(Config-If-Vlan1)#ip ospf authentication md5 123abc 1

20.4.2.2.7 ip ospf cost

命令：**ip ospf cost <*cost*>**

no ip ospf cost

功能：指定接口运行 OSPF 协议所需的代价；本命令的 no 操作为恢复缺省值。

参数：**<*cost* >**为 OSPF 协议所需花费的值，取值范围 1～65535。

缺省情况：接口缺省的 OSPF 协议所需花费的值为 1。

命令模式：接口配置模式

举例：将接口 vlan1 的 OSPF 路由代价配置成 3。

Switch(Config-If-Vlan1)#ip ospf cost 3

20.4.2.2.8 ip ospf dead-interval

命令：**ip ospf dead-interval <*time* >**

no ip ospf dead-interval

功能：指定相邻三层交换机路由失效的时间长度；本命令的 no 操作为恢复缺省值。

参数：**<*time* >**为相邻三层交换机失效的时间长度，单位为秒，取值范围 1～65535。

缺省情况：三层交换机失效的时间长度缺省为 40 秒（通常是 hello-interval 的 4 倍）。

命令模式：接口配置模式

使用指南：当三层交换机在 **dead-interval** 时间间隔内没有接收到来自邻居三层交换机的 HELLO 数据包，则认为该三层交换机不可达、失效。本命令可以根据链路的实际情况修改相邻三层交换机路由失效时间的值。设置的 **dead-interval** 的值将写入 Hello 报文中，并随 Hello 报文传送。为使 OSPF 协议的正常运行，必须保证和该接口相邻的三层交换机之间的 **dead-interval** 参数一致，且至少为 **hello-interval** 值的 4 倍。

举例：将接口 vlan1 的 OSPF 路由失效时间设置为 80s。

Switch(Config-If-Vlan1)#ip ospf dead-interval 80

20.4.2.2.9 ospf enable area

命令：**ip ospf enable area <*area_id*>**

no ip ospf enable area

功能：配置接口属于某个 OSPF 区域；本命令的 no 操作为取消该配置。

参数：**<*area_id*>**为该接口所属区域的区域号，取值范围 0～4294967295。

缺省情况：接口缺省没有被配置成属于某个区域。

命令模式：接口配置模式

使用指南：要在某一个接口上运行 OSPF 协议，必须首先指定该接口属于一个区域。

举例：将接口 vlan1 配置为属于 1 域。

Switch(Config-If-Vlan1)#ip ospf enable area 1

20.4.2.2.10 ip ospf hello-interval

命令：**ip ospf hello-interval <*time*>**

no ip ospf hello-interval

功能：指定在接口上发送 HELLO 报文的时间间隔；本命令的 no 操作为恢复缺省值。

参数：**<*time*>**为发送 HELLO 报文的时间间隔，单位为秒，取值范围 1～255。

缺省情况：接口缺省发送 HELLO 报文的间隔时间为 10 秒。

命令模式：接口配置模式

使用指南：HELLO 数据包是一种最常见的一种数据包，它周期性地被发送至邻接三层交换机，用于发现和维持邻接关系、选举 DR 与 BDR。用户设置的 **hello-interval** 的值将写入 HELLO 报文中，并随 HELLO 报文传送。**hello-interval** 的值越小，则网络拓扑结构的变化将被越快的发现，同时路由开销也增加。为使 OSPF 协议的正常运行，必须保证和该接口相邻的三层交换机之间的 **hello-interval** 参数一致。

举例：配置接口 vlan1 发送 HELLO 报文的间隔时间为 20 秒。

Switch(Config-If-Vlan1)#ip ospf hello-interval 20

相关命令：ip ospf dead-interval

20.4.2.2.11 ip ospf passive-interface

命令：ip ospf passive-interface

no ip ospf passive-interface

功能：将接口设置为只收不发 OSPF 报文；本命令的 no 操作为取消该项配置。

缺省情况：接口缺省状态是收发 OSPF 报文。

命令模式：接口配置模式

举例：配置以太网口接口 vlan1 只收不发 OSPF 报文。

Switch(Config-If-Vlan1)#ip ospf passive-interface

20.4.2.2.12 ip ospf priority

命令：ip ospf priority <*priority*>

no ip ospf priority

功能：配置接口在选举"指定三层交换机"（DR）时的优先级；本命令的 no 操作为恢复缺省值。

参数：<*priority*>为优先级，合法的取值范围是 0～255。

缺省情况：接口在选举指定三层交换机时缺省的优先级值为 1。

命令模式：接口配置模式

使用指南：当连在同一网段的两台三层交换机都想成为"指定三层交换机"时，根据优先级的值来决定谁是"指定三层交换机"，通常选择优先级高的作为"指定三层交换机"；如果优先级值相等，则选 router-id 号大的。当一台三层交换机的优先级值为 0 时，这台三层交换机将不会被选举为"指定三层交换机"或"备份指定三层交换机"。

举例：配置接口在选举指定三层交换机 DR 中的优先级。将接口 vlan1 配置成没有选举权利，即 priority 值为 0。

Switch(Config-If-Vlan1)#ip ospf priority 0

20.4.2.2.13 ip ospf retransmit-interval

命令：ip ospf retransmit-interval <*time*>

no ip ospf retransmit-interval

功能：指定接口与邻接三层交换机之间传送链路状态宣告（LSA）时的重传间隔；本命令的 no 操作为恢复缺省值。

参数：<*time*>为与邻接三层交换机之间传送链路状态宣告时的重传间隔，单位为秒，取值

范围 1～65535。
缺省情况：缺省重传间隔为 5 秒。
命令模式：接口配置模式
使用指南：当一台三层交换机向它的邻居传送链路状态宣告时，它将保持链路状态宣告直至收到对方的确认，若在时间间隔内没有收到确认报文，则三层交换机将重传链路状态宣告。重传间隔的值必须大于两台三层交换机传送报文一个来回的时间。
举例：设置接口 vlan1 重传 lsa 的时间为 10 秒。
Switch(Config-If-Vlan1)#ip ospf retransmit 10

20.4.2.2.14 ip ospf transmit-delay

命令：ip ospf tranmsit-delay <*time*>
no ip ospf transmit-delay
功能：设置在接口上传送链路状态宣告（LSA）的时延值；本命令的 no 操作为恢复缺省值。
参数：<*time*>为接口上传送链路状态宣告的时延值，单位为秒，取值范围 1～65535。
缺省情况：接口上传送链路状态宣告的缺省时延值为 1 秒。
命令模式：接口配置模式
使用指南：链路状态宣告在本三层交换机中会随时间老化，但在网络传输过程中却不会，因此在发送链路状态宣告之前增加 **transmit-delay** 的时延，使之能在老化之前将链路状态宣告发送出去。
举例：设置接口 vlan1 发送 LSA 的时延为 2 秒。
Switch(Config-If-Vlan1)#ip ospf transmit-delay 2

20.4.2.2.15 network

命令：network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]
no network <*network*> <*mask*> area <*area_id*>
功能：为三层交换机的各个网络定义所属区域；本命令的 no 操作为删除该项配置。
参数：<*network*>和**<*mask*>**为网络 IP 地址和地址通配符位，点分十进制格式；**<*area_id*>**为区域号，取值范围 0～4294967295；**advertise | notadvertise** 指定是否将到这一网络范围路由的摘要信息广播出去。
缺省情况：系统缺省没有配置网络所属的区域；若配置了，则缺省认为是广播摘要信息。
命令模式：OSPF 协议配置模式
使用指南：一旦将某一网络的范围加入到区域中，所有该网络的内部路由都不再被独立地广播到别的区域，而只是广播整个网络范围路由的摘要信息。引入网络范围和对该范围的限定，可以减少区域间路由信息的交流量。

举例：定义网络范围 10.1.1.0 255.255.255.0 加入到区域 1 中。
Switch(Config-Router-Ospf)#network 10.1.1.0 255.255.255.0 area 1

20.4.2.2.16 preference

命令：preference [ase] <*preference* >
no preference [ase]

功能：配置 OSPF 协议在各路由协议之间的
优先级，以及引入的自治系统外部路由的优先级；本命令的 no 操作为恢复缺省值。
参数：ase 表示指定引入自治系统外部路由的优先级；***<preference >***为优先级值，取值范围 1～255。
缺省情况：OSPF 协议的缺省优先级为 110；引入的外部路由协议的缺省优先级为 150。
命令模式：OSPF 协议配置模式
使用指南：由于三层交换机上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。所以为每一种路由协议指定了一个缺省的优先级，当不同协议发现同一条路由时，优先级高的协议将起决定作用。优先级更改后对新构造的路由开始有效。由 OSPF 的性质决定，OSPF 的优先级不宜过低。
举例：设置 OSPF 引入 ase 路由时的优先级为 20。
Switch(Config- Router-Ospf)#preference ase 20

20.4.2.2.17 redistribute ospfase

命令：redistribute ospfase { bgp |connected | static | rip} [type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>]
no redistribute ospfase { bgp |connected | static | rip}
功能：引入 **bgp 路由、直连路由、静态路由和** RIP 路由作为外部路由信息；本命令的 no 操作为取消引入的外部路由信息。
参数：bgp 表示引入 BGP 路由作为外部路由信息；**connected** 表示引入直连路由作为外部路由信息；**static** 表示引入静态路由作为外部路由信息；**rip** 表示引入 RIP 协议发现路由作为外部路由信息；**type** 指定外部路由类型，**1 | 2** 分别表示第一类外部路由和第二类外部路由；**tag** 指定路由的标记，***<tag>***为路由的标记值，取值范围为 0～4294967295；**metric** 指定路由的权值，***<cost_value>***为路由的权值，取值范围为 1～16777215。
缺省情况：OSPF 缺省不引入外部路由。
命令模式：OSPF 协议配置模式
使用指南：三层交换机上各动态路由协议之间是可以互相共享路由信息的，由于 OSPF 的特性，其它的路由协议发现的路由总被当作自治系统外部的路由信息处理。
举例：在 OSPF 路由中引入 RIP 路由作为第一类外部路由，引入标记值为 3，引入代价为 20。
Switch(Config-Router-Ospf)#redistribute ospfase rip type 1 tag 3 metric 20

20.4.2.2.18 router id

命令：router id <*router_id*>
no router id
功能：配置运行 OSPF 协议三层交换机的 ID 号；本命令的 no 操作为取消三层交换机的 ID 号。
参数：*<router_id>*为三层交换机 ID 号，点分十进制格式。
缺省情况：系统缺省为不配置三层交换机 ID 号，协议运行时从各接口的 IP 地址中选其中一个地址作为三层交换机 ID 号。
命令模式：全局配置模式
使用指南：OSPF 协议运行时把三层交换机的 ID 号作为本三层交换机在自治系统中的唯一

标识，通常选取三层交换机中运行 OSPF 协
议的某个接口的 IP 地址作为 ID 号。神州数码三层交换机缺省使用该交换机的最先 UP 起来的三层接口的 IP 地址为 router id。若三层交换机所有接口上都没有配置 IP 地址时，必须使用本命令指定三层交换机的 ID 号，否则 OSPF 协议无法运行。三层交换机 ID 号的变化在 OSPF 重启后才起作用。

举例：指定三层交换机的 ID 号为 10.1.120.1。

Switch(Config)#router id 10.1.120.1

20.4.2.2.19 router ospf

命令：router ospf

no router ospf

功能：启动 OSPF 协议的，开启后进入 OSPF 模式；本命令的 no 操作为关闭 OSPF 协议。

缺省情况：系统缺省不运行 OSPF 协议。

命令模式：全局配置模式

使用指南：使用本命令运行或终止 OSPF 协议。有关 OSPF 的配置，只有在系统运行了 OSPF 后才能生效。

举例：配置本交换机运行 OSPF。

Switch(Config)#router ospf

20.4.2.2.20 stub cost

命令：stub cost <*cost*> area <*area_id* >

no stub area <*area_id* >

功能：将一个区域定义成 STUB 区域；本命令的 no 操作为取消该定义。

参数：<*cost*>为 stub 区域缺省路由的花费值，取值范围 1～65535；**<*area_id* >**为 stub 区域的区域号，取值范围 1～4294967295。

缺省情况：系统缺省没有配置 STUB 区域。

命令模式：OSPF 协议配置模式

使用指南：当一个区域只有一个出口点时（只与一个三层交换机相连），或不必为每个外部目的地选择出口点时，它就可以被配置成 STUB 域。在 STUB 区域中类型 4LSA（ASBR 汇总 LSA）和类型 5LSA（AS 外部 LSA）等两种 LSA 不允许泛滥进入/通过，可以节省该区域内部各三层交换机处理外部路由信息所花费的资源。

举例：将 1 域配置成 STUB 域，缺省路由的代价为 60。

Switch(Config-Router-Ospf)#stub cost 60 area 1

20.4.2.2.21 virtuallink neighborid

命令：virtuallink neighborid <*router_id*> transitarea <*area_id*> [hellointerval <*time*>] [deadinterval <*time*>] [retransmit<*time*>] [transitdelay <*time*>]

no virtuallink neighborid <*router_id*> transitarea <*area_id*>

功能：创建并配置虚连接；本命令的 no 操作删除一条虚连接。

参数：<*router_id*>为虚连接邻居的 ID，点分十进制格式；**<*area_id*>**为转换区域的区域号，取值范围 0～4294967295；其余四项可选时间间隔配置参数同 OSPF 接口配置模式下的命

令。

缺省情况：系统缺省没有配置虚连接。

命令模式：OSPF 协议配置模式

使用指南：引入虚连接的概念是为了实现或者增强骨干区域（area 0）的连通性。由于骨干区域必须在逻辑上保持连通，因此，如果出现在骨干区域上两个节点之间没有一条区域内部路由的情况，就应该在这两个节点之间穿过某一转换区域（Transit Area）建立虚连接。虚连接由对端三层交换机的 ID 号来标识。为虚连接两端提供一条非骨干区域内部路由的区域称为转换区域，其区域号也必须在配置时指明。

虚连接在穿过转换区域的路由计算出来后被激活，相当于在两个端点之间形成了一个点到点的连接，因此，在这个连接上，和物理接口一样可以配置接口的各个参数，如 HELLO 间隔等。

举例：配置通过转换区域 2 到达 11.1.1.1 的虚连接。

Switch(Config-Router-Ospf)#virtuallink neighborid 11.1.1.1 transitarea 2

20.4.2.2.22 show ip ospf

命令：show ip ospf

功能：显示 OSPF 主要信息。

缺省情况：不显示。

命令模式：特权用户配置模式

举例：

```
Switch#show ip ospf
my router ID is 11.11.4.1
preference=10     ase perference=150
export metric=1
export tag=-2147483648
area ID   0
    interface count：1
    80times spf has been run for this area
    net range：
LSRefreshTime is1800
area ID   1
    interface count：1
    41times spf has been run for this area
    net range：
netid11.11.3.255     netaddress11.11.0.0     netmask255.255.252.0
LSRefreshTime is1800
```

显示信息	解释
my router ID	本三层交换机的 ID 号；
preference	路由协议的优先级；
ase perference	引入外部路由的优先级；
export metric	从端口输出的度量值
export tag	从端口输出的路由标记
area ID	OSPF 区域号码：包括域内的接口数的统计

interface count imes spf has been run for this area net range	值、SPF 算法的运算次数的统计、网络范围的统计等等。

20.4.2.2.23 show ip ospf ase

命令：show ip ospf ase
功能：显示 OSPF 外部路由信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：

```
Switch#show ip ospf ase
Destination    AdvRouter   NextHop   Age  SeqNumber    Type   Cost
10.1.1.125     11.11.1.2   11.1.1.2   3   300          2      20
```

显示信息	解释
Destination	目标网段或地址；
AdvRouter	选举路由；
NextHop	下一跳地址；
Age	老化时间；
SeqNumber	序列号；
Type	引入外部路由的类型；
Cost	引入外部路由的花费.

20.4.2.2.24 show ip ospf cumulative

命令：show ip ospf cumulative
功能：显示 OSPF 统计信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：

```
Switch#show ip ospf cumulative
IO cumulative
type         in        out
HELLO        1048      253
DD           338       337
LS Req       62        219
LS Update    753       295
LS Ack       495       308
ASE count    0         checksum   0
original  LSA  340   LS_RTR  179   LS_NET  1   LS_SUM_NET  160   LS_SUM_ASB  0
LS_ASE 0
```

received LSA 325
Areaid 0
nbr count 1   interface count 1
spf times 120
DB entry count 6
LS_RTR 2 LS_NET 2 LS_SUM_NET 3 LS_SUM_ASB 0 LS_ASE 3
Areaid 1
nbr count 2   interface count 1
spf times 52
DB entry count 6
LS_RTR 3 LS_NET 3 LS_SUM_NET 1 LS_SUM_ASB 0 LS_ASE 3
AS internal route 4   AS external route 0

显示信息	解释
IO cumulative	输入输出 OSPF 数据包的统计；
type	数据包类型：包括 hello 报文、DD 报文、LS 的请求、更新、确认包等；
In	输入统计值；
Out	输出统计值；
Areaid	具体针对 OSPF 的某个区域的 OSPF 数据统计。

20.4.2.2.25 show ip ospf database

命令：**show ip ospf database [{asb-summary| external | network | router | summary}]**
功能：显示 OSPF 连接状态数据库信息。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：根据本命令的输出信息，可以查看 OSPF 连接状态数据库信息。
举例：
Switch#show ip ospf database
OSPF router ID：11.11.4.1   AS：No
Area 1>>>>>>>> Area ID： 0
Router LSAs

LS ID (Router ID)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215
Router LSA					
11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Network

LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(DR's IP)					
11.11.4.2	11.11.4.2	1	2147483662	1	35126

Summary Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Net's IP)					
11.11.1.0	11.11.4.1	0	2147483656	1	6777215
11.11.2.255	11.11.4.1	0	2147483649	1	6777215
11.11.3.255	11.11.4.1	0	2147483680	1	6777215

ASBR Summary LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(ASBR's Rtr ID)					

Area 2>>>>>>>> Area ID： 1

Router LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Router ID)					
11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875
Router LSA					
11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875

Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(DR's IP)					
11.11.1.1	11.11.4.1	0	2147483649	1	6777215
11.11.1.3	14.14.14.1	15	2147483705	1	53384

Summary Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Net's IP)					
11.11.4.255	11.11.4.1	0	2147483677	1	6777215

ASBR Summary LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(ASBR's Rtr ID)					

AS External LSAs

LS ID	Route type	ADV rtr	Age	Sequence	Cost	Checksu	Forw addr	RouteTag
(Ext Net's IP)								

显示信息	解释
OSPF router ID	三层交换机的 ID；
Area 1>>>>>>>> Area ID： 0	表示从区域1到区域0各项LSA数据库信息；
Router LSAs	路由 LSA；
Network LSAs	网络 LSA；
Summary Network LSAs	汇总网络 LSA；
ASBR Summary LSAs	自治系统外部 LSA。

20.4.2.2.26 show ip ospf interface

命令：show ip ospf interface <*interface*>
功能：显示 OSPF 接口信息。
参数：<*interface*>为接口名。
缺省情况：不显示
命令模式：特权用户配置模式
举例：

Switch#show ip ospf interface vlan 1
IP address： 11.11.4.1 Mask： 255.255.255.0 Area： 0
Net type： BROADCAST cost： 1
State： IBACKUP Type： BDR
Priority： 1 Transit Delay： 1
DR： 11.11.4.2 BDR： 11.11.4.1
Authentication key：
Timer： Hello：10 Poll： 0 Dead： 40 Retrans： 5
Number of Neigbors： 1 Nubmer of Adjacencies： 1
Adjacencies：
 1： 11.11.4.2

显示信息	解释
IP address	接口的 IP 地址；
Mask	接口掩码；
Area	接口所属区域；
Net type	网络类型，如广播、点对多点等；
cost	花费值；
State	状态；
Type	三层交换机类型，如是否是指定三层交换机；
Priority	在选举指定三层交换机中的优先级；
Transit Delay	接口传送 LAS 的延时值；
DR	指定三层交换机；
BDR	备份指定三层交换机；
Authentication key	OSPF 报文认证密钥；
Timer： Hello、Poll、Dead、Retrans	OSPF 协议计时器：包括 hello 报文、pollinterval 报文、路由失效、路由重发等的

	时间值；
Number of Neigbors	相邻三层交换机的个数；
Nubmer of Adjacencies	相邻路由接口的个数；
Adjacencies	相邻接口的 IP 地址；

20.4.2.2.27 show ip ospf neighbor

命令：show ip ospf neighbor
功能：显示 OSPF 邻接点信息。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：根据本命令输出信息，可以查看 OSPF 邻居的情况。
举例：

```
Switch#show ip ospf neighbor
interface ip 12.1.1.1      area id 0
   router id 12.1.1.2       router ip addr 12.1.1.2
   state NFULL      priority 1
   DR 12.1.1.2       BDR 12.1.1.1
   last hello 59006      last exch 49717
interface ip 30.1.1.1      area id 0
interface ip 50.1.1.1      area id 0
   router id 50.1.1.2       router ip addr 50.1.1.2
   state NFULL      priority 0
   DR 50.1.1.1       BDR 0.0.0.0
   last hello 59010      last exch 49614
interface ip 51.1.1.1      area id 0
interface ip 52.1.1.1      area id 0
interface ip 100.1.1.1      area id 0
interface ip 110.1.1.1      area id 0
interface ip 150.1.1.1      area id 0
   router id 12.2.0.0       router ip addr 150.1.1.2
   state NFULL      priority 0
   DR 150.1.1.1       BDR 0.0.0.0
   last hello 59011      last exch 49607
```

显示信息	解释
interface ip	本三层交换机某一接口 IP 地址
area id	接口所属区域号；
router id	相邻三层交换机的 ID 号；
router ip addr	相邻三层交换机的接口的 IP 地址；
state	链路状态；
priority	优先级；
DR	指定三层交换机 ID；

BDR	备份指定三层交换机 ID；
last hello	最后的 hello 报文；
last exch	最后的交换报文。

20.4.2.2.28 show ip ospf routing

命令：show ip ospf routing
功能：显示 OSPF 路由表信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：

```
Switch#show ip ospf routing
AS internal routes：
Destination      Area    Cost    Dest Type    Next Hop      ADV rtr
60.2.127.0       0       7       DTYPE_NET    12.1.1.2      6.1.1.2
60.1.132.0       0       7       DTYPE_NET    12.1.1.2      6.1.1.2
60.4.67.0        0       7       DTYPE_NET    12.1.1.2      6.1.1.2
60.3.72.0        0       7       DTYPE_NET    12.1.1.2      6.1.1.2
60.2.77.0        0       7       DTYPE_NET    12.1.1.2      6.1.1.2
AS external routes：
Destination      Cost    Dest Type       Next Hop         ADV rtr
```

显示信息	解释
AS internal routes	自治系统内部路由；
AS external routes	自治系统外部路由；
Destination	目标网段；
Area	区域号；
Cost	花费值；
Dest Type	路由类型；
Next Hop	下一跳；
ADV rtr	通告三层交换机接口地址

20.4.2.2.29 show ip ospf virtual-links

命令：show ip ospf virtual-links
功能：显示 OSPF 虚连接信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：

```
Switch#show ip ospf virtual-links
no virtual-link
```

20.4.2.2.30 show ip protocols

命令：**show ip protocols**
功能：显示三层交换机当前运行路由协议的信息。
命令模式：特权用户配置模式
使用指南：根据本命令的输出信息，用户可以确认配置是否正确和进行路由故障诊断。
举例：

```
Switch#sh ip protocols
OSPF is running.
my router ID is 100.1.1.1
preference=10     ase perference=150
export metric=1
export tag=-2147483648
area ID   1
interface count:2
7times spf has been run for this area
net range:
LSRefreshTime is1800
RIP information
rip is shutting down
```

显示信息	解释
OSPF is running	正在运行的路由协议为 OSPF 协议；
My router ID	运行 OSPF 协议三层交换机的 ID 号；
Preference	OSPF 路由的优先级；
Ase perference	自治系统外部路由的优先级；
Export metric	输出 OSPF 路由的度量值；
Export tag	输出 OSPF 路由的标签值；
Area ID	三层交换机所在 OSPF 域的 ID 号；
Interface count	运行 OSPF 路由协议的接口数；
N times spf has been run for this area	三层交换机进行最小生成树的计算；
Net range	运行 OSPF 协议的网络区间；
LSRefreshTime	OSPF 协议刷新链路状态通告 LSA 周期时间。

20.4.2.2.31 debug ip ospf event

命令：**debug ip ospf event**
　　　no debug ip ospf event
功能：打开显示 OSPF 的各种事件信息的调试开关；本命令是 no 操作为关闭本调试开关。
缺省情况：调试开关关闭。
命令模式：特权用户配置模式

20.4.2.2.32　debug ip ospf lsa

命令：**debug ip ospf lsa**
　　　no debug ip ospf lsa
功能：打开显示链路状态宣告信息的调试开关；本命令的 no 操作为关闭本调试开关。
缺省情况：调试开关关闭。
命令模式：特权用户配置模式

20.4.2.2.33　debug ip ospf packet

命令：**debug ip ospf packet**
　　　no debug ip ospf packet
功能：打开显示 OSPF 报文信息的调试开关；本命令的 no 操作为关闭本调试开关。
缺省情况：调试开关关闭。
命令模式：特权用户配置模式
举例：

```
Switch#debug ip ospf packet
packet length：  44
02：40：54：
receive ACK from 11.11.1.3
02：40：56：
receive a packet from 11.11.1.2
packet length：  44
02：40：56：
receive ACK from 11.11.1.2
02：40：58：
receive a packet from 11.11.4.2
packet length：  48
02：40：58：
receive a HELLO packet from 11.11.4.2 via Broadcast interface 11.11.4.1
02：40：58：
```

20.4.2.2.34　debug ip ospf spf

命令：**debug ip ospf spf**
　　　no debug ip ospf spf
功能：打开显示 OSPF 有关最短路径算法信息的调试开关；本命令的 no 操作关闭本调试开关。
缺省情况：调试开关关闭。
命令模式：特权用户配置模式

20.4.3　OSPF 典型案例

案例一：OSPF自治系统

以五台神州数码三层交换机为例组成一个OSPF自治系统，其中三层交换机SWITCH1和SWITCH5组成OSPF 0域，三层交换机SWITCH2和SWITCH3组成OSPF 1域（设三层交换机SWITCH1的vlan 1接口属于0域），三层交换机SWITCH4组成OSPF 2域（设三层交换机SWITCH5的vlan 2接口属于0域）。SWITCH1和SWITCH5为骨干三层交换机，SWITCH2和SWITCH4为域边界三层交换机，SWITCH3为域内部三层交换机。

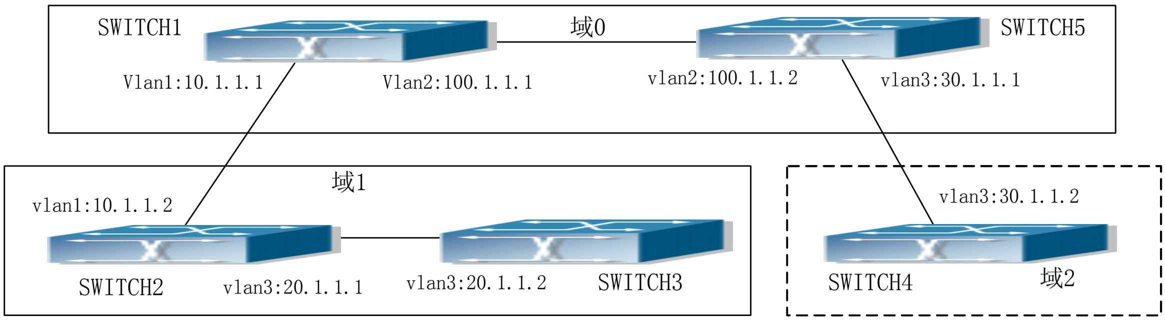


图 20-3 OSPF自治系统网络拓扑示意图

三层交换机SWITCH1- SWITCH5的配置分别如下：

三层交换机SWITCH1：

!配置接口vlan1的IP地址。

SWITCH1#config

SWITCH1(config)# interface vlan 1

SWITCH1(config-if-vlan1)# ip address 10.1.1.1 255.255.255.0

SWITCH1(config-if-vlan1)#no shut-down

SWITCH1(config-if-vlan1)#exit

! 配置接口vlan2的IP地址

SWITCH1(config)# interface vlan 2

SWITCH1(config-if-vlan2)# ip address 100.1.1.1 255.255.255.0

SWITCH1 (config-if-vlan2)#exit

！ 启动OSPF协议，配置接口vlan1、vlan2所属域号

SWITCH1(config)#router ospf

SWITCH1(config-router-ospf)#exit

SWITCH1(config)#interface vlan 1

SWITCH1 (config-if-vlan1)#ip ospf enable area 0

SWITCH1 (config-if-vlan1)#exit

SWITCH1(config)#interface vlan2

SWITCH1 (config-if-vlan2)#ip ospf enable area 0

SWITCH1 (config-if-vlan2)#exit

SWITCH1(config)#exit

SWITCH1#

三层交换机SWITCH2：

!配置接口vlan1和vlan2的IP地址。

SWITCH2#config

SWITCH2(config)# interface vlan 1

SWITCH2(config-if-vlan1)# ip address
10.1.1.2 255.255.255.0
SWITCH2(config-if-vlan1)#no shut-down
SWITCH2(config-if-vlan1)#exit
SWITCH2(config)# interface vlan 3
SWITCH2(config-if-vlan3)# ip address 20.1.1.1 255.255.255.0
SWITCH2(config-if-vlan3)#no shut-down
SWITCH2(config-if-vlan3)#exit
！启动OSPF协议，配置接口vlan1和vlan3所属OSPF区域
SWITCH2(config)#router ospf
SWITCH2(config-router-ospf)#exit
SWITCH2(config)#interface vlan 1
SWITCH2(config-if-vlan1)#ip ospf enable area 0
SWITCH2(config-if-vlan1)#exit
SWITCH2(config)#interface vlan 3
SWITCH2(config-if-vlan3)#ip ospf enable area 1
SWITCH2(config-if-vlan3)#exit
SWITCH2(config)#exit
SWITCH2#
三层交换机SWITCH3：
!配置接口vlan3的IP地址。
SWITCH3#config
SWITCH3(config)# interface vlan 3
SWITCH3(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0
SWITCH3(config-if-vlan3)#no shut-down
SWITCH3(config-if-vlan3)#exit
！启动OSPF协议，配置接口vlan3所属OSPF区域
SWITCH3(config)#router ospf
SWITCH3(config-router-ospf)#exit
SWITCH3(config)#interface vlan 3
SWITCH3(config-if-vlan3)#ip ospf enable area 1
SWITCH3(config-if-vlan3)#exit
SWITCH3(config)#exit
SWITCH3#
三层交换机SWITCH4：
!配置接口vlan3的IP地址。
SWITCH4#config
SWITCH4(config)# interface vlan 3
SWITCH4(config-if-vlan3)# ip address30.1.1.2 255.255.255.0
SWITCH4(config-if-vlan3)#no shut-down
SWITCH4(config-if-vlan3)#exit
！启动OSPF协议，配置接口vlan3所属OSPF区域
SWITCH4(config)#router ospf
SWITCH4(config-router-ospf)#exit

SWITCH4(config)#interface vlan 3
SWITCH4(config-if-vlan3)#ip ospf enable area 0
SWITCH4(config-if-vlan3)#exit
SWITCH4(config)#exit
SWITCH4#
三层交换机SWITCH5：
!配置接口vlan2的IP地址。
SWITCH5#config
SWITCH5(config)# interface vlan 2
SWITCH5(config-if-vlan2)# ip address 30.1.1.1 255.255.255.0
SWITCH5(config-if-vlan2)#no shut-down
SWITCH5(config-if-vlan2)#exit
！配置接口vlan3的IP地址
SWITCH5(config)# interface vlan 3
SWITCH5(config-if-vlan3)# ip address 100.1.1.2 255.255.255.0
SWITCH5(config-if-vlan3)#no shut-down
SWITCH5(config-if-vlan3)#exit
！启动OSPF协议，配置接口vlan2和vlan3所属域号
SWITCH5(config)#router ospf
SWITCH5(config-router-ospf)#exit
SWITCH5(config)#interface vlan 2
SWITCH5(config-if-vlan2)#ip ospf enable area 0
SWITCH5(config-if-vlan2)#exit
SWITCH5(config)#interface vlan 3
SWITCH5(config-if-vlan3)#ip ospf enable area 0
SWITCH5(config-if-vlan3)#exit
SWITCH5(config)#exit
SWITCH5#

案例二：OSPF协议典型复杂拓扑

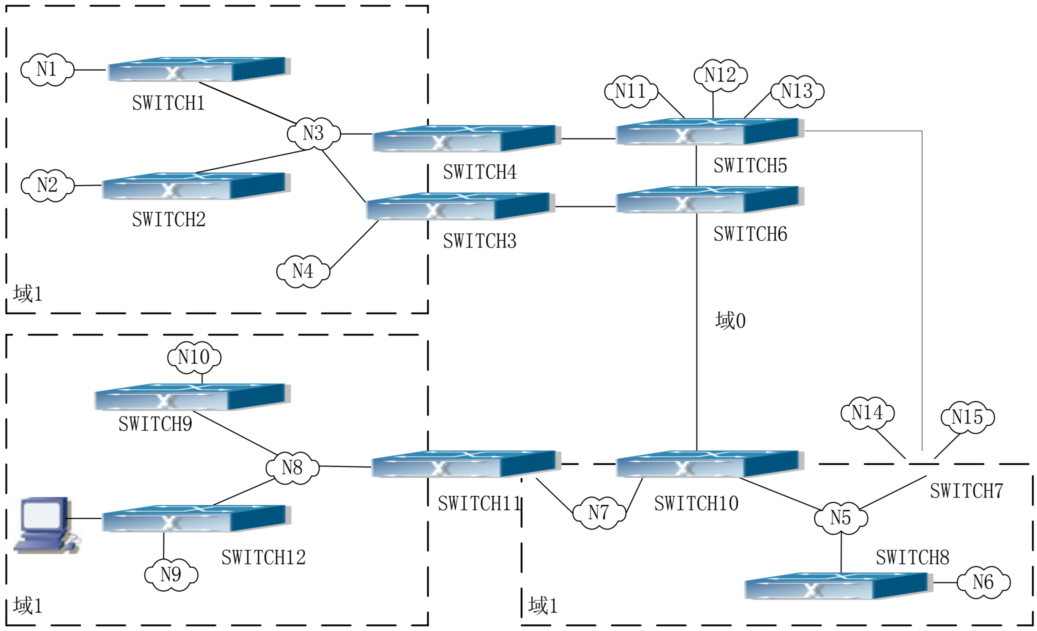


图 20-4 复杂典型 OSPF 自治系统

图5.2.5为一个典型复杂的OSPF自治系统网络拓扑。域1包括网络N1-N4和三层交换机SWITCH1-SWITCH4，域2包括网络N5-N7和三层交换机SWITCH7、SWITCH8、SWITCH10和SWITCH11，域3包括N8-N10、主机H1与三层交换机SWITCH9、 SWITCH11和SWITCH12，且配置成网络N8-N10和主机H1使用一条汇总路由（即将域3定义为STUB域）。三层交换机SWITCH1、SWITCH2、SWITCH5、SWITCH6、SWITCH8、SWITCH9和SWITCH12是域内三层交换机，三层交换机SWITCH3、SWITCH4、SWITCH7、SWITCH10和SWITCH11是域边界三层交换机，三层交换机SWITCH5和SWITCH7是自治系统边界三层交换机。

就域1而言，三层交换机SWITCH1和SWITCH2是域内三层交换机，域边界三层交换机SWITCH3和SWITCH4负责向域1通告所有到该域外目的地的距离代价，同时SWITCH3和SWITCH4还必须向域1通告自治系统边界三层交换机SWITCH5和SWITCH7的位置，来自SWITCH5和SWITCH7的自治系统外部链路状态通告在整个自治系统内泛滥。当自治系统外部链路状态通告在域1内泛滥时，这些LSA被包含在域1数据库内，从而得到到网络N11-N15的路由。

另外，三层交换机SWITCH3和SWITCH4也必须向骨干域（即0域，所有非0域必须通过0域相连，不允许它们直接相连）汇总域1的拓扑结构，通告域1所包含的网络（即N1-N4）以及从SWITCH3和SWITCH4到这些网络的代价。由于骨干域要求必须是连通的，所以在骨干三层交换机SWITCH10和SWITCH11之间必须建立一条虚链接。域边界三层交换机之间通过骨干三层交换机来交换汇总信息，每一个域边界三层交换机监听来自其它域边界三层交换机的汇总信息。

虚链路不仅用于保证骨干域的连通性，还用于健壮骨干域。比如，骨干三层交换机SWITCH6和SWITCH10之间的链路如果被切断，这将导致骨干域不连续。通过在骨干三层交换机SWITCH7和SWITCH10之间建立一条虚链路，骨干域会变得更健壮一些。同时，

SWITCH7和SWITCH10之间的虚链接提供了
到域3和三层交换机SWITCH7的一条更短的路径。

以域1为例，假设三层交换机SWITCH1的接口vlan2的IP地址为10.1.1.1；三层交换机SWITCH2的接口VLAN2的IP地址为10.1.1.2；三层交换机SWITCH3的接口VLAN2的IP地址为10.1.1.3；三层交换机SWITCH4的接口VLAN2的IP地址为10.1.1.4。SWITCH1使用以太口VLAN1与网络N1相连，IP地址为20.1.1.1；SWITCH2使用以太口VLAN1与网络N2相连，IP地址为20.1.2.1；SWITCH3使用以太口VLAN3与网络N4相连，IP地址为20.1.3.1；都属于域1。SWITCH3使用以太网口VLAN1与三层交换机SWITCH6相连，IP地址为10.1.5.1；SWITCH4使用以太网口VLAN1与三层交换机SWITCH5相连，IP地址为10.1.6.1；都属于域0。域1内的三层交换机之间采用简单密钥认证，域1边界三层交换机与域0骨干三层交换机之间采用MD5密钥认证。

下面仅给出域1内各三层交换机的配置，其他域三层交换机的配置省略。SWITCH1、SWITCH2、SWITCH3和SWITCH4的配置分别如下：

1)SWITCH1：

```
!配置接口vlan2的IP地址
SWITCH1#config
SWITCH1(config)# interface vlan 2
SWITCH1(config-If-Vlan2)# ip address 10.1.1.1 255.255.255.0
SWITCH1(config-If-Vlan2)#exit
！启动OSPF协议，配置接口vlan2所属域号
SWITCH1(config)#router ospf
SWITCH1(config-router-ospf)#exit
SWITCH1(config)#interface vlan 2
SWITCH1(config-If-Vlan2)#ip ospf enable area 1

!配置简单密钥认证
SWITCH1(config-If-Vlan2)#ip ospf authentication simple DCS
SWITCH1(config-If-Vlan2)exit
!配置接口vlan1的IP地址,配置所属域号
SWITCH1(config)# interface vlan 1
SWITCH1(config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
SWITCH1(config-If-Vlan1)#ip ospf enable area 1
SWITCH1(config-If-Vlan1)#exit
```

2)SWITCH2：

```
!配置接口vlan2的IP地址
SWITCH2#config
SWITCH2(config)# interface vlan 2
SWITCH2(config-If-Vlan2)# ip address 10.1.1.2 255.255.255.0
SWITCH2(config-If-Vlan2)#exit
！启动OSPF协议，配置接口vlan2所属域号
SWITCH2(config)#router ospf
SWITCH2(config-router-ospf)#exit
SWITCH2(config)#interface vlan 2
SWITCH2(config-If-Vlan2)#ip ospf enable area 1
```

!配置简单密钥认证
SWITCH2(config-If-Vlan2)#ip ospf authentication simple DCS
SWITCH2(config-If-Vlan2)#exit
!配置接口vlan1的IP地址，配置所属域号
SWITCH2(config)# interface vlan 1
SWITCH2(config-If-Vlan1)#ip address 20.1.2.1 255.255.255.0
SWITCH2(config-If-Vlan1)#ip ospf enable area 1
SWITCH2(config-If-Vlan1)#exit
SWITCH2(config)#exit
SWITCH2#
3)SWITCH3：
!配置接口vlan2的IP地址
SWITCH3#config
SWITCH3(config)# interface vlan 2
SWITCH3(config-If-Vlan2)# ip address 10.1.1.3 255.255.255.0
SWITCH3(config-If-Vlan2)#exit
！启动OSPF协议，配置接口vlan2所属域号
SWITCH3(config)#router ospf
SWITCH3(config-router-ospf)#exit
SWITCH3(config)#interface vlan 2
SWITCH3(config-If-Vlan2)#ip ospf enable area 1
!配置简单密钥认证
SWITCH3(config-If-Vlan2)#ip ospf authentication simple DCS
SWITCH3(config-If-Vlan2)#exit
!配置接口vlan3的IP地址，配置所属域号
SWITCH3(config)# interface vlan 3
SWITCH3(config-If-Vlan3)#ip address 20.1.3.1 255.255.255.0
SWITCH3(config-If-Vlan3)#ip ospf enable area 1
SWITCH3(config-If-Vlan3)#exit
!配置接口vlan1的IP地址，并配置接口所属域号
SWITCH3(config)# interface vlan 1
SWITCH3(config-If-Vlan1)#ip address 10.1.5.1 255.255.255.0
SWITCH3(config-If-Vlan1)#ip ospf enable area 0
!配置MD5密钥认证
SWITCH3 (config-If-Vlan1)#ip ospf authentication md5 DCS
SWITCH3 (config-If-Vlan1)#exit
SWITCH3(config)#exit
SWITCH3#
4)SWITCH4：
!配置接口vlan2的IP地址
SWITCH4#config
SWITCH4(config)# interface vlan 2
SWITCH4(config-If-Vlan2)# ip address 10.1.1.4 255.255.255.0
SWITCH4(config-If-Vlan2)#exit

！启动OSPF协议，配置接口vlan2所属域
号
SWITCH4(config)#router ospf
SWITCH4(config-router-ospf)#exit
SWITCH4(config)#interface vlan 2
SWITCH4(config-If-Vlan2)#ip ospf enable area 1
!配置简单密钥认证
SWITCH4(config-If-Vlan2)#ip ospf authentication simple DCS
SWITCH4(config-If-Vlan2)#exit
!配置接口vlan1的IP地址，并配置接口所属域号
SWITCH4(config)# interface vlan 1
SWITCH4(config-If-Vlan1)# ip address 10.1.6.1 255.255.255.0
SWITCH4(config-If-Vlan1)#ip ospf enable area 0
!配置MD5密钥认证
SWITCH4(config-If-Vlan1)#ip ospf authentication md5 DCS
SWITCH4(config-If-Vlan1)exit
SWITCH4(config)#exit
SWITCH4#

20.4.4 OSPF 排错帮助

1.监测和调试命令
2.OSPF 排错帮助

20.4.4.1 监测和调试命令

命令	解释
特权用户配置模式	
Show interface	显示接口信息，保证接口和链路层协议 UP。
Show ip ospf	显示 OSPF 当前运行状态及配置信息。根据该命令的输出信息，用户可以确认配置是否正确和进行 OSPF 故障诊断。
Show ip route	显示路由表信息，可以查看有关 OSPF 路由信息
Show ip ospf ase	显示 OSPF 外部路由信息。
Show ip ospf cumulative	显示 OSPF 统计信息。
Show ip ospf database	显示 OSPF 连接状态数据库信息。
Show ip ospf interface	显示指定接口配置的 OSPF 信息。
Show ip ospf neighbor	显示 OSPF 邻居信息。
Show ip ospf routing	显示 OSPF 路由表信息。
Show ip ospf virtual-links	显示 OSPF 虚连接信息。
Show ip protocols	显示运行的路由协议信息。

[no] debug ip ospf event	调试 OSPF 的各种事件信息；no 命令为关闭本调试开关。
[no] debug ip ospf lsa	调试链路状态宣告的信息，no 命令关闭本调试开关。
[no] debug ip ospf packet	调试 OSPF 数据报信息，no 命令关闭本调试开关。
[no] debug ip ospf spf	调试 spf 信息，no 命令关闭本调试开关。

（1）show ip ospf

举例：

Switch#show ip ospf
my router ID is 11.11.4.1
preference=10　ase perference=150
export metric=1
export tag=-2147483648
area ID　0
　interface count：1
　80times spf has been run for this area
　net range：
LSRefreshTime is1800
area ID　1
　interface count：1
　41times spf has been run for this area
　net range：
netid11.11.3.255　netaddress11.11.0.0　netmask255.255.252.0
LSRefreshTime is1800

显示信息	解释
my router ID	本三层交换机的 ID 号；
preference	路由协议的优先级；
ase perference	引入外部路由的优先级；
export metric	从端口输出的跳数；
export tag	从端口输出的路由标记
area ID interface count imes spf has been run for this area net range	OSPF 区域号码：包括域内的接口数的统计值、SPF 算法的运算次数的统计、网络范围的统计等等。

（2）show ip route

使用 show ip route 命令可以显示路由表中关于 OSPF 路由的目的 IP 地址、网络掩码以及下一跳 IP 地址或转发接口等信息。

例如，显示信息为：

Switch#show ip route
Total route items is 4018, the matched route items is 4018
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
　　A - OSPF ASE, B - BGP derived, D - DVMRP derived

```
     Destination        Mask              Nexthop           Interface        Preference
C    4.1.140.0          255.255.255.0     0.0.0.0           Vlan2139         0
A    5.1.1.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.2.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.3.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.4.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.5.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.6.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.7.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.8.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.9.0            255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.10.0           255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.11.0           255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.12.0           255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.13.0           255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.14.0           255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.15.0           255.255.255.0     12.1.1.2          Vlan12           150
A    5.1.16.0           255.255.255.0     12.1.1.2          Vlan12           150
O    5.1.17.0           255.255.255.0     12.1.1.2          Vlan12           110
---More---
```

其中，O 表示 OSPF 路由，即目的网络地址为 5.1.17.0、网络掩码为 255.255.255.0、下一跳地址为 12.1.1.2 以及转发接口为 vlan 12 的一条路由为 OSPF 路由，它的优先级为 110。

（3）show ip ospf ase

使用 show ip ospf ase 命令可以显示关于 OSPF 自治系统外部路由的信息。

例如，显示信息为：

```
Switch#show ip ospf ase
Destination    AdvRouter    NextHop    Age    SeqNumber    Type    Cost
10.1.1.125     11.11.1.2    11.1.1.2   3      300          2       20
```

显示信息	解释
Destination	目标网段或地址；
AdvRouter	选举路由；
NextHop	下一跳地址；
Age	老化时间；
SeqNumber	序列号；
Type	引入外部路由的类型；
Cost	引入外部路由的花费.

（4）show ip ospf cumulative

使用 show ip ospf cummulative 命令可以显示关于 OSPF 路由协议的统计信息。

例如，显示信息为：

```
Switch#show ip ospf cumulative
IO cumulative
type          in          out
```

HELLO 1048 253
DD 338 337
LS Req 62 219
LS Update 753 295
LS Ack 495 308
ASE count 0 checksum 0
original LSA 340 LS_RTR 179 LS_NET 1 LS_SUM_NET 160 LS_SUM_ASB 0
LS_ASE 0
received LSA 325
Areaid 0
nbr count 1 interface count 1
spf times 120
DB entry count 6
LS_RTR 2 LS_NET 2 LS_SUM_NET 3 LS_SUM_ASB 0 LS_ASE 3
Areaid 1
nbr count 2 interface count 1
spf times 52
DB entry count 6
LS_RTR 3 LS_NET 3 LS_SUM_NET 1 LS_SUM_ASB 0 LS_ASE 3
AS internal route 4 AS external route 0

显示信息	解释
IO cumulative	输入输出 OSPF 数据包的统计；
type	数据包类型：包括 hello 报文、DD 报文、LS 的请求、更新、确认包等；
In	输入统计值；
Out	输出统计值；
Areaid	具体针对 OSPF 的某个区域的 OSPF 数据统计。

（5）show ip ospf database

使用 show ip ospf database 命令可以显示关于 OSPF 路由协议的连接状态数据库信息。

例如，显示信息为：

Switch#show ip ospf database
OSPF router ID：11.11.4.1 AS：No
Area 1>>>>>>>> Area ID： 0
Router LSAs
LS ID ADV rtr Age Sequence Cost Checksum
(Router ID)
11.11.4.1 11.11.4.1 0 2147483808 0 42401
11.11.4.2 11.11.4.2 18 2147483863 1 6777215
Router LSA
11.11.4.1 11.11.4.1 0 2147483808 0 42401

11.11.4.2 11.11.4.2 18 2147483863 1 6777215

```
                              Network
LSAs
LS ID           ADV rtr         Age     Sequence        Cost    Checksum
(DR's IP)
11.11.4.2        11.11.4.2       1       2147483662      1       35126
                              Summary Network LSAs
LS ID           ADV rtr         Age     Sequence        Cost    Checksum
(Net's IP)
11.11.1.0        11.11.4.1       0       2147483656      1      6777215
11.11.2.255      11.11.4.1       0       2147483649      1      6777215
11.11.3.255      11.11.4.1       0       2147483680      1       6777215
                              ASBR Summary LSAs
LS ID          ADV rtr         Age     Sequence        Cost    Checksum
(ASBR's Rtr ID)

Area 2>>>>>>>> Area ID：  1
                              Router LSAs
LS ID          ADV rtr         Age     Sequence        Cost    Checksum
(Router ID)
11.11.2.1       11.11.2.1       1       2147483698      1       6777215
14.14.14.1      14.14.14.1      1       2147483662      1       14831
11.11.4.1       11.11.4.1       0       2147483669      0       33875
Router LSA
11.11.2.1       11.11.2.1       1       2147483698      1       6777215

14.14.14.1       14.14.14.1      1       2147483662      1       14831

11.11.4.1        11.11.4.1       0       2147483669      0       33875

                              Network LSAs
LS ID          ADV rtr         Age     Sequence        Cost    Checksum
(DR's IP)
11.11.1.1       11.11.4.1       0       2147483649      1       6777215
11.11.1.3       14.14.14.1      15      2147483705      1       53384
                              Summary Network LSAs
LS ID          ADV rtr         Age     Sequence        Cost    Checksum
(Net's IP)
11.11.4.255     11.11.4.1       0       2147483677      1       6777215
                              ASBR Summary LSAs
LS ID          ADV rtr         Age     Sequence        Cost    Checksum
(ASBR's Rtr ID)
                              AS External LSAs
LS ID   Route type ADV rtr   Age   Sequence Cost Checksu   Forw addr    RouteTag
(Ext Net's IP)
```

显示信息	解释
OSPF router ID	三层交换机的 ID；
Area 1>>>>>>>> Area ID： 0	表示从区域1到区域0各项LSA数据库信息；
Router LSAs	路由 LSA；
Network LSAs	网络 LSA；
Summary Network LSAs	汇总网络 LSA；
ASBR Summary LSAs	自治系统外部 LSA。

（6）show ip ospf interface

使用 show ip ospf interface 命令可以显示关于接口的 OSPF 路由协议信息。

例如，显示信息为：

Switch#show ip ospf interface vlan 1

IP address： 11.11.4.1 Mask： 255.255.255.0 Area： 0

Net type： BROADCAST cost： 1

State： IBACKUP Type： BDR

Priority： 1 Transit Delay： 1

DR： 11.11.4.2 BDR： 11.11.4.1

Authentication key：

Timer： Hello：10 Poll： 0 Dead： 40 Retrans： 5

Number of Neigbors： 1 Nubmer of Adjacencies： 1

Adjacencies：

1： 11.11.4.2

显示信息	解释
IP address	接口的 IP 地址；
Mask	接口掩码；
Area	接口所属区域；
Net type	网络类型，如广播、点对多点等；
cost	代价值；
State	状态；
Type	三层交换机类型，如是否是指定三层交换机；
Priority	在选举指定三层交换机中的优先级；
Transit Delay	接口传送 LAS 的延时值；
DR	指定三层交换机；
BDR	备份指定三层交换机；
Authentication key	OSPF 报文认证密钥；
Timer： Hello、Poll、Dead、Retrans	OSPF 协议计时器：包括 hello 报文、pollinterval 报文、路由失效、路由重发等的时间值；
Number of Neigbors	相邻三层交换机的个数；
Nubmer of Adjacencies	相邻路由接口的个数；
Adjacencies	相邻接口的 IP 地址；

（7）show ip ospf neighbor

使用 show ip ospf neighbor 命令可以显示关于 OSPF 邻居三层交换机的信息。

例如，显示信息为：

```
Switch#show ip ospf neighbor
interface ip 12.1.1.1        area id 0
   router id 12.1.1.2        router ip addr 12.1.1.2
   state NFULL        priority 1
   DR 12.1.1.2        BDR 12.1.1.1
   last hello 66261        last exch 65712
interface ip 30.1.1.1        area id 0
interface ip 50.1.1.1        area id 0
   router id 50.1.1.2        router ip addr 50.1.1.2
   state NFULL        priority 0
   DR 50.1.1.1        BDR 0.0.0.0
   last hello 66286        last exch 49614
interface ip 51.1.1.1        area id 0
interface ip 52.1.1.1        area id 0
interface ip 100.1.1.1        area id 0
interface ip 110.1.1.1        area id 0
interface ip 150.1.1.1        area id 0
   router id 12.2.0.0        router ip addr 150.1.1.2
   state NFULL        priority 0
   DR 150.1.1.1        BDR 0.0.0.0
   last hello 66289        last exch 49607
```

显示信息	解释
interface ip	本三层交换机某一接口 IP 地址
area id	接口所属区域号；
router id	相邻三层交换机的 ID 号；
router ip addr	相邻三层交换机的接口的 IP 地址；
state	链路状态；
priority	优先级；
DR	指定三层交换机 ID；
BDR	备份指定三层交换机 ID；
last hello	最后的 hello 报文；
last exch	最后的交换报文。

（8）show ip ospf routing

使用 show ip ospf routing 命令可以显示关于 OSPF 路由表的信息。

例如，显示信息为：

```
Switch#show ip ospf routing
AS internal routes：
Destination        Area      Cost      Dest Type    Next Hop        ADV rtr
11.11.1.0          1         1          0         11.11.1.1       14.14.14.1
11.11.4.0          0         1          0         11.11.4.1       11.11.4.2
11.11.2.0          1         2          0         11.11.1.2       11.11.2.1
11.11.3.0          1         11         0         11.11.1.3       14.14.14.1
AS external routes：
Destination        Cost      Dest Type          Next Hop         ADV rtr
```

显示信息	解释
AS internal routes	自治系统内部路由；
AS external routes	自治系统外部路由；
Destination	目标网段；
Area	区域号；
Cost	代价值；
Dest Type	路由类型；
Next Hop	下一跳；
ADV rtr	通告三层交换机接口地址

（9）show ip ospf virtual-links

使用 show ip ospf virtual-links 命令可以显示关于 OSPF 虚链路信息。

例如，显示信息为：

Switch#show ip ospf virtual-links

no virtual-link

（10）show ip protocols

使用 show ip protocols 命令可以显示当前三层交换机运行路由协议的信息。

例如，显示信息为：

Switch#sh ip protocols

OSPF is running.

my router ID is 100.1.1.1

preference=10   ase perference=150

export metric=1

export tag=-2147483648

area ID   1

interface count:2

7times spf has been run for this area

net range:

LSRefreshTime is1800

RIP information

rip is shutting down

显示信息	解释
OSPF is running	正在运行的路由协议为 OSPF 协议；
My router ID	运行 OSPF 协议三层交换机的 ID 号；
Preference	OSPF 路由的优先级；
Ase perference	自治系统外部路由的优先级；
Export metric	输出 OSPF 路由的度量值；
Export tag	输出 OSPF 路由的标签值；
Area ID	三层交换机所在 OSPF 域的 ID 号；
Interface count	运行 OSPF 路由协议的接口数；
N times spf has been run for this area	三层交换机进行最小生成树的计算；
Net range	运行 OSPF 协议的网络区间；
LSRefreshTime	OSPF 协议刷新链路状态通告 LSA 周期时间。

第21章组播协议配置

21.1 组播协议概述

21.1.1 组播简介

当信息（包括数据、语音和视频）传送的目的地是网络中的少数用户时，可以采用多种传送方式。可以采用单播（Unicast）的方式，即为每个用户单独建立一条数据传送通路；或者采用广播（Broadcast）的方式，把信息传送给网络中的所有用户，不管他们是否需要，都会接收到广播来的信息。例如，在一个网络上有200个用户需要接收相同的信息时，传统的解决方案是用单播方式把这一信息分别发送200次，以便确保需要数据的用户能够得到所需的数据；或者采用广播的方式，在整个网络范围内传送数据，需要这些数据的用户可直接在网络上获取。这两种方式都浪费了大量宝贵的带宽资源，而且广播方式也不利于信息的安全和保密。

IP组播技术的出现及时解决了这个问题。组播源仅发送一次信息，组播路由协议为组播数据包建立树型路由，被传递的信息在尽可能远的分叉路口才开始复制和分发，因此，信息能够被准确高效地传送到每个需要它的用户。

需要注意的是，组播源不一定需要加入组播组，它向某些组播组发送数据，自己不一定是该组的接收者。可以同时有多个源向一个组播组发送报文。网络中可能有不支持组播的路由器，组播路由器可以使用隧道方式将组播包封装在单播IP包中传送给相邻的组播路由器，相邻的组播路由器再将单播IP头剥掉，然后继续进行组播传输。从而避免对网络的结构进行较大的改动。组播的优势主要在于：

1) 提高效率：降低网络流量，减轻服务器和CPU负荷；
2) 优化性能：减少冗余流量；
3) 分布式应用：使多点应用成为可能。

21.1.2 组播地址

组播报文的目的地址使用D类IP地址， 范围是从224.0.0.0到239.255.255.255。D类地址不能出现在IP报文的源IP地址字段。单播数据传输过程中，一个数据包传输的路径是从源地址路由到目的地址，利用“逐跳”（hop-by-hop）的原理在IP网络中传输。然而在IP组播环境中，数据包的目的地址不是一个，而是一组，形成组地址。所有的信息接收者都加入到一个组内，并且一旦加入之后，流向组地址的数据立即开始向接收者传输，组中的所有成员都能接收到数据包。组播组中的成员是动态的，主机可以在任何时刻加入和离开组播组。

组播组可以是永久的也可以是临时的。组播组地址中，有一部分由官方分配的，称为永久组播组。永久组播组保持不变的是它的IP地址，组中的成员构成可以发生变化。永久组播组中成员的数量都可以是任意的，甚至可以为零。那些没有保留下来供永久组播组使用的IP

组播地址，可以被临时组播组利用。

224.0.0.0～224.0.0.255为预留的组播地址（永久组地址），地址224.0.0.0保留不做分配，其它地址供路由协议使用； 224.0.1.0～238.255.255.255为用户可用的组播地址（临时组地址），全网范围内有效；239.0.0.0～239.255.255.255为本地管理组播地址，仅在特定的本地范围内有效。常用的预留组播地址列表如下：

224.0.0.0 基准地址（保留）

224.0.0.1 所有主机的地址

224.0.0.2 所有组播路由器的地址

224.0.0.3 不分配

224.0.0.4 DVMRP 路由器

224.0.0.5 OSPF 路由器

224.0.0.6 OSPF DR

224.0.0.7 ST 路由器

224.0.0.8 ST 主机

224.0.0.9 RIP-2 路由器

224.0.0.10 IGRP 路由器

224.0.0.11 活动代理

224.0.0.12 DHCP 服务器/中继代理

224.0.0.13 所有PIM 路由器

224.0.0.14 RSVP 封装

224.0.0.15 所有CBT 路由器

224.0.0.16 指定SBM

224.0.0.17 所有SBMS

224.0.0.18 VRRP

以太网传输单播IP报文的时候，目的MAC地址使用的是接收者的MAC地址。但是在传输组播报文时，传输目的不再是一个具体的接收者，而是一个成员不确定的组，所以使用的是组播MAC地址。组播MAC地址是和组播IP地址对应的。IANA（Internet Assigned Number Authority）规定，组播MAC地址的高24bit为0x01005e，MAC 地址的低23bit为组播IP地址的低23bit。

由于IP组播地址的后28位中只有23位被映射到MAC地址，这样就会有32个IP组播地址映射到同一MAC地址上。

21.1.3 IP 组播报文转发

在组播模型中，源主机向IP数据包目的地址字段内的组播组地址所表示的主机组传送信息。和单播模型不同的是，组播模型必须将组播数据包转发到多个外部接口上以便能传送到所有接收站点，因此组播转发过程比单播转发过程更加复杂。

为了保证组播信息包都是通过最短路径到达路由器，组播必须依靠单播路由表或者单独提供给组播使用的单播路由表（如DVMRP路由表），对组播信息包的接收接口进行一定的检查，这种检查机制就是大部分组播路由协议进行组播转发的基础——RPF（Reverse Path Forwarding，逆向路径转发）检查。组播路由器利用到达的组播数据包的源地址来查询单播路由表或者独立的组播路由表，以确定此数据包到达的入接口处于接收站点至源地址的最短

路径上。如果使用的是有源树，这个源地址就
是发送组播数据包的源主机的地址；如果使用的是共享树，该源地址就是共享树的根的地址。当组播数据包到达路由器时，如果RPF 检查通过，数据包则按照组播转发项进行转发，否则，数据包被丢弃。

21.1.4 IP 组播应用

IP组播技术有效地解决了单点发送多点接收的问题，实现了IP网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。利用网络的组播特性可以方便地提供一些新的增值业务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视/音频会议等互联网的信息服务领域，包括：

1) 多媒体、流媒体的应用；
2) 数据仓库、金融应用（股票）等；
3) 任何“点到多点”的数据发布应用。

在IP 网络中多媒体业务日渐增多的情况下，组播有着巨大的市场潜力，组播业务也将逐渐得到推广和普及。

21.2 组播公共配置

21.2.1 组播公共配置命令

- **show ip mroute**

21.2.1.1 show ip mroute

命令：show ip mroute [*group_address*] [*source_address*]
功能：显示 ip 组播报文转发项。
参数：[*group_address*] 限定显示转发项的组地址；**[*source_address*]** 限定显示转发项的源地址。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：本命令用于显示 ip 组播转发项，即系统 FIB 表中用于转发组播报文的转发项。
举例： 显示所有 ip 组播转发项
Switch # **show ip mroute**
Name: Loopback, Index: 27, State:9 localaddr: 127.0.0.1, remote: 127.0.0.1
Name: Vlan1, Index: 29, State:13 localaddr: 1.1.1.1, remote: 1.1.1.1
Name: Vlan4, Index: 52, State:13 localaddr: 2.1.1.1, remote: 2.1.1.1
Name: Vlan3, Index: 40, State:13 localaddr: 3.1.1.1, remote: 3.1.1.1
Group   Origin   Iif   Wrong   Oif:TTL

```
225.1.1.101         1.1.1.100           Vlan1
0          52:1
                                                                    40:1
239.255.0.1        9.1.1.100          Vlan4             0          29:1
239.255.0.1        7.1.1.100          Vlan4             0          29:1
239.255.0.1        1.1.1.100          Vlan1               0          52:1
                                                                    40:1
Switch #
```

显示信息	解释
Name	列出组播协议使用的接口列表，并描述接口的基本信息
Index	接口的索引号
Group	组播转发项组地址
Origin	组播转发项源地址
Iif	组播转发项入接口
Wrong	从错误入接口收到的组播报文（对该转发项）计数
Oif:TTL	Oif 出接口列表，使用接口索引号，可以通过上面给出的接口列表与接口索引号对应；TTL 为该出接口上的 TTL 门限值

21.3 PIM-DM

21.3.1 PIM-DM 介绍

PIM-DM（Protocol Independent Multicast，Dense Mode，协议独立组播－密集模式）属于密集模式的组播路由协议，适用于小型网络，在这种网络环境下，组播组的成员相对比较密集。

PIM-DM 的工作过程可以概括为：邻居发现、扩散—剪枝过程、嫁接阶段。

1. 邻居发现

PIM-DM 路由器刚开始启动时，需要使用Hello报文来发现邻居。运行PIM-DM的各网络节点之间使用Hello报文保持联系。PIM-DM Hello报文是周期性发送的。

2. 扩散—剪枝过程（Flooding&Prune）

PIM-DM 假设网络上的所有主机都准备接收组播数据。当某组播源S开始向组播组G发送数据时，在路由器接收到组播报文后，首先根据单播路由表进行RPF检查，如果检查通过，路由器创建一个（S，G）表项，然后将组播报文向网络上所有下游PIM-DM节点转发（Flooding）。如果没有通过RPF检查，即组播报文是从错误的接口输入，则将该报文丢弃。经过这个过程，在PIM-DM组播域内，每个节点都会创建一个（S，G）表项。如果下游节点没有组播组成员，则向上游节点发剪枝（Prune）消息，通知上游节点不用再转发该组播组数据。上游节点收到剪枝消息后，就将相应的接口从其组播转发表项（S，G）对应的输出接口列表中删除，这就建立了一个以源S为根的SPT（Shortest Path Tree，SPT）树。剪枝过程最先由叶子路由器发起。

上述过程就称为扩散—剪枝过程。各个被剪枝的节点同时提供超时机制，当剪枝超时时，路由器重新开始扩散—剪枝过程。PIM-DM的扩散—剪枝机制周期性进行。

3. RPF检查

PIM-DM采用RPF检查，利用现存的单播路由表构建一棵从数据源始发的组播转发树。当一个组播包到达时，路由器首先判断到达路径的正确性。如果到达接口是单播路由指示的通往组播源的接口，就认为这个组播包是从正确路径而来；否则，将组播包作为冗余报文丢弃。作为路径判断依据的单播路由信息可以来源于任何一种单播路由协议，如RIP、OSPF 等发现的路由信息，而不依赖于特定的单播路由协议。

4. Assert机制

如果处于一个LAN网段上的两台组播路由器A和B，各自有到组播源S的接收途径，它们在接收到组播源S发出的组播数据报文以后，都会向LAN上转发该组播报文，这时，下游节点组播路由器C就会收到两份相同的组播报文。路由器检测到这种情况后，需要通过Assert机制来选定一个唯一的转发者。通过发送Assert报文，选出一条最优的转发路径，如果两条或两条以上路径的优先级和开销相同，则选择IP地址大的节点作为该（S，G）项的上游邻居，由它负责该（S，G）组播报文的转发。

5. 嫁接（Graft）

当被剪枝的下游节点需要恢复到转发状态时，该节点使用嫁接报文通知上游节点恢复组播数据转发。

21.3.2 PIM-DM 配置

21.3.2.1 PIM-DM 配置任务序列

1、 启动 PIM-DM（必须）

2、 配置 PIM-DM 辅助参数（可选）

配置 PIM-DM 接口参数

配置 PIM-DM hello 报文间隔时间

1. 启动 PIM-DM 协议

在 DCRS 系列三层交换机上运行 PIM-DM 路由协议的基本配置很简单，只需在相应接口下打开 PIM-DM 开关即可。

命令	解释
接口配置模式	
[no] ip pim dense-mode	启动 PIM-DM 协议，本命令的 no 操作关闭 PIM-DM 协议。（必须）

2. 配置 PIM-DM 辅助参数

（1）配置 PIM-DM 接口参数

1）配置 PIM-DM hello 报文间隔时间

命令	解释
接口配置模式	
ip pim query-interval <*query interval*> **no ip pim query-interval**	配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

3. 关闭 **PIM-DM** 协议

命令	解释
接口配置模式	
no ip pim dense-mode	关闭 PIM-DM 协议。

21.3.2.2 PIM-DM 的配置命令

- **ip pim dense-mode**
- **ip pim query-interval**
- **show ip pim interface**
- **show ip pim mroute dm**
- **show ip pim neighbor**
- **debug ip pim**

21.3.2.3 ip pim dense-mode

命令：ip pim dense-mode
no ip pim dense-mode
功能：在接口上启动 PIM-DM 协议；本命令的 no 操作在接口上关闭 PIM-DM 协议。
参数：无。
缺省情况：缺省为不启动 PIM-DM 协议。
命令模式：接口配置模式
使用指南：
举例：在接口 vlan1 上启动 PIM-DM 协议。
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip pim dense-mode

21.3.2.4 ip pim query-interval

命令：ip pim query-interval <*query interval*>
no ip pim query-interval
功能：配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。
参数：<*query interval*>为周期发送 PIM-DM hello 报文的时间间隔，取值范围 1～18724s。
缺省情况：周期发送 PIM-DM hello 报文的时间间隔缺省为 10s。
命令模式：接口配置模式
使用指南：hello 消息使得 PIM-DM 交换机可以互相定位，确定邻居关系。PIM-DM 交换机通过周期向邻居发送 hello 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的 hello 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。
举例：在接口 vlan1 上配置 PIM-DM hello 间隔。
Switch (Config)#interface vlan1
Switch(Config-If-Vlan1)#ip pim query-interval 20

21.3.3 PIM-DM 典型案例

如下图，将 SwitchA，switchB 的以太网接口加入到相应的 vlan 中，并在各 vlan 接口上启动 PIM-DM 协议

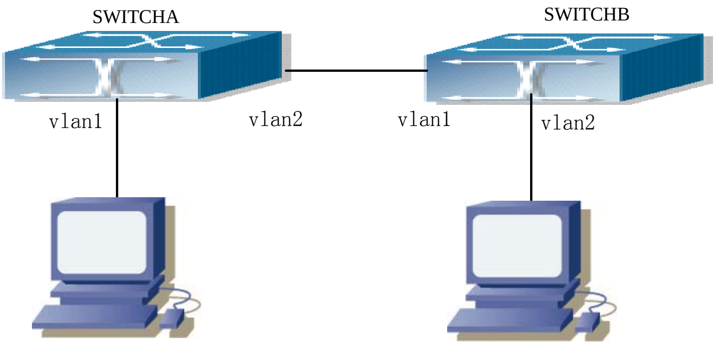


图 21-1 PIM-DM 典型环境

SWITCHA 和SWITCHB配置步骤如下：

(1) 配置SWITCHA：

Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim dense-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan2
Switch(Config-If-Vlan1)# ip pim dense-mode

(2) 配置SWITCHB：

Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim dense-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan1)# ip pim dense-mode

21.3.4 PIM-DM 排错帮助

1.监测和调试命令
2.PIM-DM 排错帮助

21.3.4.1 监测和调试命令

命令	解释
特权用户配置模式	
show ip pim mroute dm	显示 PIM-DM 报文转发项

show ip pim neighbor	显示 PIM-DM 邻居信息
show ip pim interface	显示 PIM-DM 接口信息
debug ip pim	打开显示 pim 详细信息的调试开关；本命令的 no 操作为关闭本调试开关

21.3.4.2 show ip pim mroute dm

命令：show ip pim mroute dm
功能：显示 PIM-DM 报文转发项。
参数：无。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：本命令用于显示 PIM-DM 组播转发项，即系统 FIB 表中用于转发组播报文的转发项。
举例： 显示所有 PIM-DM 报文转发项

```
Switch#sh ip pim mroute dm

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
          Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
          Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

PIMDM Group Table, inodes 7 routes 4:

(5.1.1.100, 225.0.0.1), protos: 0x8, flags: 0x4, 00:22:21/00:03:30
  Incoming interface : Vlan3, RPF Nbr 0.0.0.0, pref 0, metric 0
  Outgoing interface list:
          (Vlan1), protos: 0x2, UpTime: 00:22:21, Exp:/
  Prune interface list:
          (Vlan2), protos: 0x2, UpTime: 00:22:21, Exp: 00:03:07

(5.1.1.100, 225.0.0.2), protos: 0x8, flags: 0x4, 00:18:52/00:03:30
  Incoming interface : Vlan3, RPF Nbr 0.0.0.0, pref 0, metric 0
  Outgoing interface list:
          (Vlan1), protos: 0x2, UpTime: 00:18:52, Exp:/
  Prune interface list:
          (Vlan2), protos: 0x2, UpTime: 00:18:52, Exp: 00:02:51
Switch#
```

显示信息	解释
(5.1.1.100, 225.0.0.1)	转发项
Incoming interface	入接口，即 RPF 接口
Outgoing interface list	出接口列表
Prune interface list	下游剪枝接口列表

21.3.4.3 show ip pim neighbor

命令：show ip pim neighbor [<*ifname*>]
功能：显示 pim 接口上的邻居信息。
参数：**<*ifname*>**为接口名称，即显示指定接口上的 pim 邻居信息。
缺省情况：显示所有接口上的 pim 邻居信息。
命令模式：特权用户配置模式
使用指南：如果不输入接口名，则显示所有接口上的 pim 邻居信息。
举例：显示在所有接口（不输入接口名）上的 pim 邻居信息。

```
Switch#sh ip pim neighbor
Neighbor-Address Interface          ifIndex Uptime     Expires   DR-state
 2.1.1.1              Vlan1         2005       00:25:17 00:01:15 /
 9.1.1.6              Vlan2         2006       00:25:09 00:01:35 DR
 5.1.1.4              Vlan3         2007       00:25:01 00:01:38 DR
Switch#
```

显示信息	解释
Neighbor-Address	邻居地址
Interface	发现该邻居接口
ifIndex	接口索引号
Uptime	该邻居已存在的时间
Expires	该邻居距离超时还剩的时间
DR-state	该邻居是否 DR

21.3.4.4 show ip pim interface

命令：show ip pim interface [<*ifname*>]
功能：显示 pim 接口信息。
参数：**<*ifname*>**为接口名称，即显示指定接口上的 pim 信息。
缺省情况：显示所有接口的 pim 信息。
命令模式：特权用户配置模式
举例：显示在接口 vlan1 上的 pim 信息。

```
Switch#sh ip pim interface vlan 1
Interface Vlan1 : 2.1.1.2
 owner is pimdm, Vif is 1, Hello Interval is 30
 Neighbor-Address Interface          Uptime     Expires
 2.1.1.1              Vlan1         00:26:23 00:01:39
Switch#
```

显示信息	解释
Interface（上面）	接口名以及接口 ip
Owner	接口所属组播路由协议
Vif	接口对应的虚接口索引
Hello Interval	接口配置的 hello 报文间隔（单位秒）
Neighbor-Address	邻居地址

Interface（下面）	发现该邻居接口
Uptime	该邻居已存在的时间
Expires	该邻居距离超时还剩的时间

21.3.4.5 debug ip pim

- 命令：**debug ip pim**

功能：打开显示 pim 详细信息的调试开关；本命令的 no 操作为关闭本调试开关。
参数：无。
缺省情况：关闭。
命令模式：特权用户配置模式
使用指南：如果需要查看 pim 报文等的详细信息，则可以打开本调试开关。
举例：
Switch # **debug ip pim**
00:15:45: PIM: Send v2 Hello on vlan1, holdtime 105
00:15:45: PIM: Send v2 Hello on vlan1, holdtime 105
00:15:45: PIM: Received v2 Hello on vlan1 from 2.1.1.2, holdtime 105

21.3.4.6 PIM-DM 排错帮助

在配置、使用 PIM-DM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-DM 协议未能正常运行。因此，用户应注意以下要点：
- ✧ 首先应该保证物理连接的正确无误；
- ✧ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ✧ 然后，在接口上启动 PIM-DM 协议（使用 ip pim dense-mode 命令）；
- ✧ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性；

如果使用检查都尝试仍无法解决 PIM-DM 的问题，那么请使用 debug ip pim 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给神州数码技术服务中心。

21.4 PIM-SM

21.4.1 PIM-SM 介绍

PIM-SM（Protocol Independent Multicast，Sparse Mode）即与协议无关的组播稀疏模式，属于稀疏模式的组播路由协议，主要用于组成员分布相对分散、范围较广、大规模的网络。与密集模式的扩散—剪枝不同，PIM-SM协议假定所有的主机都不需要接收组播数据包，只有主机明确指定需要时，PIM-SM路由器才向它转发组播数据包。

PIM-SM通过设置汇聚点RP（Rendezvous Point）和自举路由器BSR（Bootstrap Router），向所有PIM-SM路由器通告组播信息，并利用路由器的加入/剪枝信息，建立起基于RP的共享树RPT（RP-rooted shared tree）。从而减少数据报文和控制报文占用的网络

带宽，降低路由器的处理开销。组播数据沿着
共享树流到该组播组成员所在的网段，当数据流量达到一定程度，组播数据流可以切换到基于源的最短路径树SPT，以减少网络延迟。PIM-SM不依赖于特定的单播路由协议，而是使用现存的单播路由表进行RPF检查。

1. PIM-SM工作原理

PIM-SM的工作过程主要有：邻居发现、RP共享树（RPT）的生成、组播源注册、SPT切换等。其中，邻居发现机制与PIM-DM相同，这里不再介绍。

(1) RP共享树（RPT）的生成

当主机加入一个组播组G时，与该主机直接相连的叶子路由器通过IGMP报文了解到有组播组G的接收者，就为组播组G计算出对应的汇聚点RP，然后向朝着RP方向的上一级节点发送加入组播组的消息（join 消息）。从叶子路由器到RP之间途经的每个路由器都会在转发表中生成（*，G）表项，表示由任意源发出的，发送至组播组G的，都适用于该表项。当RP收到发往组播组G的报文后，报文就会沿着已经建立好的路径到达叶子路由器，进而到达主机。这样就生成了以RP为根的RPT。

(2) 组播源注册

当组播源S向组播组G发送了一个组播报文时，与其直接相连的PIM-SM组播路由器接收到该报文以后，就负责将该组播报文封装成注册报文，单播给对应的RP。如果一个网段上有多个PIM-SM组播路由器，这时候将由指定路由器DR（Designated Router）负责发送该组播报文。

(3) SPT切换

当组播路由器发现从RP发来的目的地址为G的组播报文的速率超过了阈值时，组播路由器就向朝着源S的上一级节点发送加入消息，导致RPT向SPT的切换。

2. PIM-SM 配置前准备工作

(1) 配置候选RP

在PIM-SM网络中，可以存在多个RP（候选RP），每个候选RP（Candidate-RP，C-RP）负责转发目的地址在一定范围内的组播报文。配置多个候选RP可以实现RP负载分担。候选RP之间没有主次之分，所有的组播路由器收到BSR通告的候选RP消息后，根据相同的算法计算出与某一组播组对应的RP。

注意，一个RP可以为多个组播组服务，也可以为所有组播组服务。每个组播组在任意时刻，只能唯一地对应一个RP，不能同时对应多个RP。

(2) 配置BSR

BSR 是PIM-SM 网络里的管理核心，它负责收集候选RP发来的信息，并把它们广播出去。

一个网络内部只能有一个BSR，但可以配置多个候选BSR（Candidate-BSR， C-BSR）。这样，一旦某个BSR发生故障后，能够切换到另外一个。C-BSR通过自动选举产生BSR。

21.4.2 PIM-SM 配置

21.4.2.1 PIM-SM 配置任务序列

1、 启动 PIM-SM（必须）

2、 配置 PIM-SM 辅助参数（可选）

（1）配置 PIM-SM 接口参数
1）配置 PIM-SM hello 报文间隔时间
2）配置接口为 PIM-SM 域边界
（2） 配置 PIM-SM 全局参数
1) 配置交换机作为候选 BSR
2) 配置交换机作为候选 RP
3、关闭 PIM-SM 协议

1. 启动 PIM-SM 协议

在 DCRS 系列三层交换机上运行 PIM-SM 路由协议的基本配置很简单，只需在相应接口下打开 PIM-SM 开关即可。

命令	解释
接口配置模式	
[no] ip pim sparse-mode	启动 PIM-SM 协议，本命令的 no 操作关闭 PIM-SM 协议。（必须）

2. 配置 PIM-SM 辅助参数

（1）配置 PIM-SM 接口参数

1）配置 PIM-SM hello 报文间隔时间

命令	解释
接口配置模式	
ip pim query-interval <*query interval*> **no ip pim query-interval**	配置接口 PIM-SM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

2) 配置接口为 PIM-SM BSR 边界

命令	解释
接口配置模式	
ip pim bsr-border **no ip pim bsr-border**	配置接口为 PIM-SM BSR 边界；本命令的 no 操作为取消 BSR 边界的设置。

（2）配置 PIM-SM 全局参数

1) 配置交换机作为候选 BSR

命令	解释
接口配置模式	
ip pim bsr-candidate <*ifname*> [*hashlength*] [*Priority*] **no ip pim bsr-candidate**	该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器；本命令的 no 操作为取消候选 BSR 的配置。

2) 配置交换机作为候选 RP

命令	解释
接口配置模式	

ip pim rp-candidate <*ifname*> [group-list *access-list*] [interval *interval*] **no ip pim rp-candidate [<*ifname*>]**	该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器；本命令的 no 操作为取消候选 RP 的配置。

3. 关闭 **PIM-SM** 协议

命令	解释
接口配置模式	
no ip pim sparse-mode	关闭 PIM-SM 协议。

21.4.2.2 PIM-SM 的配置命令

- **ip pim sparse-mode**
- **ip pim bsr-border**
- **ip pim query-interval**
- **ip pim bsr-candidate**
- **ip pim rp-candidate**
- **show ip pim bsr-router**
- **show ip pim interface**
- **show ip pim mroute sm**
- **show ip pim neighbor**
- **show ip pim rp**
- **debug ip pim**
- **debug ip pim bsr**

21.4.2.2.1ip pim sparse-mode

命令：**ip pim sparse-mode**
no ip pim sparse-mode
功能：在接口上启动 PIM-SM 协议；本命令的 no 操作在接口上关闭 PIM-SM 协议。
参数：无。
缺省情况：缺省为不启动 PIM-SM 协议。
命令模式：接口配置模式
使用指南：
举例：在接口 vlan1 上启动 PIM-SM 协议。
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip pim sparse-mode

21.4.2.2.2ip pim bsr-border

命令：ip pim bsr-border

no ip pim bsr-border

功能：该命令为接口 BSR 边界配置命令，用于配置 PIM-SM 域的边界，以防止 BSR 消息的向本 PIM-SM 域外扩散；本命令的 no 操作为取消 BSR 边界的设置。

参数：无。

缺省情况：接口关闭 BSR 边界的设置。

命令模式：接口配置模式

使用指南：该命令为接口 BSR 边界配置命令，用于配置 PIM-SM 域的边界，以防止 BSR 消息的向本 PIM-SM 域外扩散,即本 PIM-SM 域内的 BSR 消息不用从这个接口向外传递；若取消 BSR 边界的设置，则需取消该配置命令。

举例：在接口 Vlan1 上启动 BSR 边界配置。

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim bsr-border

21.4.2.2.3ip pim query-interval

命令：ip pim query-interval <*query interval*>

no ip pim query-interval

功能：配置接口 pim hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

参数：<*query interval*>为周期发送 pim hello 报文的时间间隔，取值范围 1～18724s。

缺省情况：周期发送 pim hello 报文的时间间隔缺省为 30s。

命令模式：接口配置模式

使用指南：hello 消息使得 pim 交换机可以互相定位，确定邻居关系。pim 交换机通过周期向邻居发送 hello 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的 hello 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。

举例：在接口 vlan1 上配置 PIM-SM hello 间隔。

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim query-interval 20

21.4.2.2.4ip pim bsr-candidate

命令：ip pim bsr-candidate <*ifname*> [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

功能：该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器；本命令的 no 操作为取消候选 BSR 的配置。

参数：*ifname*，为指定接口名；**[*hash-mask-length*]**，为指定哈希算法中掩码长度，其用于 RP 自举选择，取值范围为 0-32；**[*priority*]** ，为本候选 BSR 的 BSR 优先级，取值范围为 0-255，若不配置该参数，则本候选 BSR 的 BSR 缺省优先级为 0。

缺省情况：本交换机不是 BSR 候选路由器。

命令模式：全局配置模式

使用指南：该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器，只有配置本命令，本交换机才是 BSR 候选路由器。

举例：全局配置接口 vlan1 为候选 BSR 消息
发送接口。
Switch (Config)# ip pim bsr-candidate vlan1 30 10

21.4.2.2.5ip pim rp-candidate

命令：ip pim rp-candidate <*ifname*> [group-list *access-list*] [interval *interval*]
no ip pim rp-candidate [<*ifname*>]

功能：该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器；本命令的 no 操作为取消候选 RP 的配置。

参数：*<ifname>*为指定接口名；***access-list***，为交换机可以充当 RP 的组范围列表数，取值范围为 1-99，若不配置该参数，则缺省路由器可以充当 RP 的组范围为所有组播组；***interval*** ，为本候选 RP 发送候选 RP 报文的间隔，取值范围为 1-16383 秒。

缺省情况：本交换机不是 RP 候选路由器。

命令模式：全局配置模式

使用指南：该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器，只有配置本命令，本交换机才是 RP 候选路由器。

举例：全局配置接口 vlan1 为候选 RP 公告消息发送接口。
Switch (Config)# ip pim rp-candidate vlan1 group-list 5
Switch (Config)# access-list 5 permit 239.255.2.0 0.0.0.255

21.4.3 PIM-SM 典型案例

如下图所示，将 switchA，switchB，switchC，switchD 的以太网接口加入到相应 vlan 中，并在各 vlan 接口上启动 PIM-SM 协议

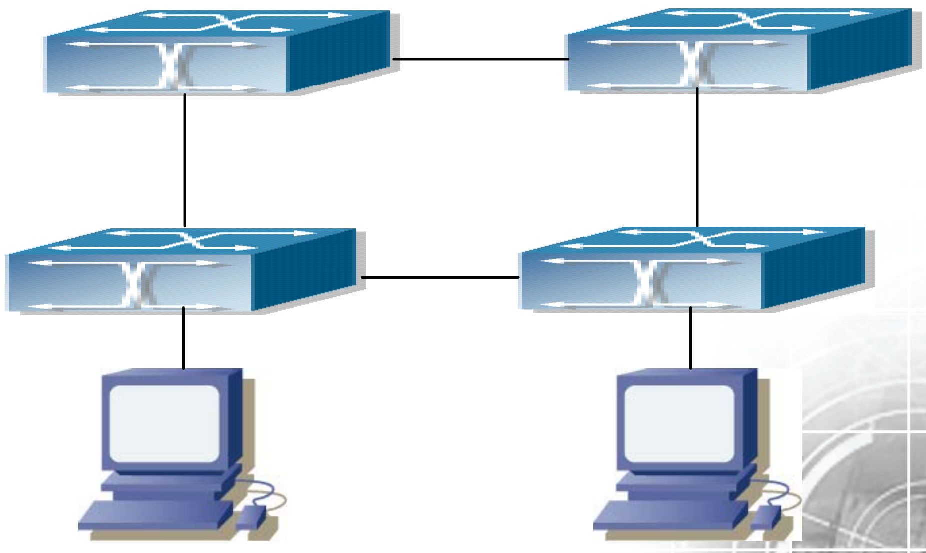


图 21-2 PIM-SM 典型环境

SWITCHA 和SWITCHB，switchC，switchD配置步骤如下：

(1) 配置SWITCHA：

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
```

(2) 配置SWITCHB：

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)# exit
Switch (Config)# ip pim rp-candidate vlan2 group-list 5
Switch (Config)# access-list 5 permit 239.255.2.0 0.0.0.255
```

(3) 配置SWITCHC：

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch (Config)# ip pim bsr-candidate vlan2 30 10
```

(4) 配置SWITCHD：

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode
```

21.4.4 PIM-SM 排错帮助

21.4.4.1 监测和调试命令

21.4.4.1.1show ip pim bsr-router

命令：show ip pim bsr-router
功能：显示 pim bsr-router 信息。
参数：无。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：显示 pim bsr-router 信息。

```
Switch #show ip pim bsr-router
Switch #
 PIMv2 Bootstrap information
  BSR address: 192.4.1.3
  Priority: 192, Hash mask length: 30
  Expires :    00:02:13.
Switch #
```

显示信息	解释
BSR address	Bsr-router 地址
Priority	Bsr-router 优先级
Hash mask length	Bsr-router 哈希掩码长度
Expires	该 Bsr-router 距离超时还剩的时间

21.4.4.1.2 show ip pim interface

命令：show ip pim interface [<*ifname*>]
功能：显示 pim 接口信息。
参数：**<*ifname*>**为接口名称，即显示指定接口上的 pim 信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：显示在接口 Vlan2 上的 pim 信息。

```
Switch #show ip pim interface vlan2
Switch #
 Interface Vlan2 : 192.3.1.2
 owner is pimsm, Vif is 1, Hello Interval is 30, pim sm jp interval is (60)
 Neighbor-Address Interface          Uptime     Expires
 192.3.1.3             Vlan2              00:12:18 00:01:38
Switch #
```

显示信息	解释
Interface（上面）	接口名以及接口 ip
owner	接口所属组播路由协议
Vif	接口对应的虚接口索引
Hello Interval	接口配置的 hello 报文间隔（单位秒）
jp interval	加入/剪枝 间隔时间
Neighbor-Address	邻居地址
Interface（下面）	发现该邻居接口
Uptime	该邻居已存在的时间
Expires	该邻居距离超时还剩的时间

21.4.4.1.3 show ip pim mroute sm

命令：**show ip pim mroute sm**
功能：显示 PIM-SM 报文转发项。
参数：无。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：本命令用于显示 PIM-SM 组播转发项，即系统 FIB 表中用于转发组播报文的转发项。
举例：

```
Switch # show ip pim mroute sm
BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
      Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
      Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;
PIMSM Group Table, inodes 1 routes 1:
(192.1.1.1, 225.0.0.1), protos: 0x8, flags: 0x0, 00:10:18/00:03:18
   Incoming interface : Vlan1, RPF Nbr 0.0.0.0, pref 0, metric 0
   Outgoing interface list:
      (Vlan2), protos: 0x2, UpTime: 00:10:18, Exp:00:03:18
Switch #
```

显示信息	解释
(192.1.1.1, 225.0.0.1)	转发项
Incoming interface	入接口，即 RPF 接口
Outgoing interface list	出接口列表

21.4.4.1.4 show ip pim neighbor

命令：**show ip pim neighbor [<*ifname*>]**
功能：显示 pim 接口上的邻居信息。
参数：**<*ifname*>**为接口名称，即显示指定接口上的 pim 邻居信息。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：如果不输入接口名，则显示所有接口上的 pim 邻居信息。
举例：显示在所有接口（不输入接口名）上的 pim 邻居信息。

```
Switch # show ip pim neighbor
  Neighbor-Address Interface        ifIndex Uptime    Expires   DR-state
  192.3.1.3        Vlan1            28      00:11:39 00:01:16 DR
  192.2.1.1        Vlan2            31      00:11:39 00:01:16 /
  192.4.1.4        Vlan4            33      00:11:39 00:01:44 DR
  192.4.1.3        Vlan4            33      00:11:39 00:01:17 /
Switch #
```

显示信息	解释
Neighbor-Address	邻居地址
Interface	发现该邻居接口
ifIndex	接口索引号
Uptime	该邻居已存在的时间
Expires	该邻居距离超时还剩的时间
DR-state	该邻居是否 DR

21.4.4.1.5show ip pim rp

命令：**show ip pim rp** [**mapping** | ***group-address***]
功能：显示 PIM 的 RP 相关信息。
参数：**mapping,** 显示组地址和 rp 的对应关系。
　　　group-address，为组地址。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：显示组 PIM 域中 226.1.1.1 的 RP 信息。
Switch #show ip pim rp 226.1.1.1
RP Address for this group is: 192.2.1.1

显示信息	解释
RP Address	本组的 rp 地址

21.4.4.1.6debug ip pim

- 命令：**debug ip pim**

功能：打开显示 pim 详细信息的调试开关；本命令的 no 操作为关闭本调试开关。
参数：无。
缺省情况：关闭。
命令模式：特权用户配置模式
使用指南：如果需要查看 pim 报文等的详细信息，则可以打开本调试开关。
举例：
Switch # debug ip pim
PIM debug is on
00:17:52: PIM: Received v2 Join/Prune on Vlan2 from 192.3.1.3 to 192.3.1.2
00:17:52: PIM: Receive Join-list: (192.1.1.1/32, 225.0.0.1/32), S-bit set
00:17:54: PIM: Received v2 Hello on Vlan4 from 192.4.1.4, holdtime 105
00:17:57: PIM: Received v2 Hello on vlan3 from 192.2.1.1, holdtime 105
00:17:57: PIM: Received v2 Hello on Vlan2 from 192.3.1.3, holdtime 105
00:17:58: PIM: Received v2 Hello on Vlan4 from 192.4.1.3, holdtime 105
00:18:21: PIM: Send v2 Hello on vlan2, holdtime 105
00:18:21: PIM: Send v2 Hello on vlan4, holdtime 105
00:18:21: PIM: Send v2 Hello on vlan3, holdtime 105
00:18:21: PIM: Send v2 Hello on Vlan4, holdtime 105

00:18:21: PIM: Send v2 Hello on Vlan2,
holdtime 105

21.4.4.1.7debug ip pim bsr

- 命令：**debug ip pim bsr**

功能：打开显示 PIM Candidate-RP/BSR 信息的调试开关；本命令的 no 操作为关闭本调试开关。
参数：无。
缺省情况：关闭。
命令模式：特权用户配置模式
使用指南：如果需要查看 PIM Candidate-RP/BSR 报文等的详细信息，则可以打开本调试开关。
举例：
Switch # debug ip pim bsr
PIM BSR debug is on
00:16:23: PIM: Received v2 BSR on Vlan4 from 192.4.1.3
00:16:23: PIM: Receive BSR fragtag 6879, hmlen: 30, pri: 192
00:16:23: PIM: Receive BSR Group (225.0.0.1, 0.0.0.0): rpcount: 1, fragcount: 1
00:16:23: PIM: C-RP 192.2.1.1, holdtime 130, C-RP pri 192
00:16:23: PIM: Transmit the BSR message on Vlan2
00:16:23: PIM: Transmit the BSR message on vlan4
00:16:23: PIM: Transmit the BSR message on vlan3
00:16:23: PIM: Transmit the BSR message on vlan2

21.4.4.2 PIM-SM 排错帮助

在配置、使用 PIM-SM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-SM 协议未能正常运行。因此，用户应注意一下要点：

- ✧ 首先应该保证物理连接的正确无误；
- ✧ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ✧ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性；
- ✧ PIM-SM 协议需要有 rp 和 bsr 的支持，所以首先使用 **show ip pim bsr-router**，看是否有 bsr 信息，如果不存在，则需要查看是否有通向 bsr 的单播路由；
- ✧ 使用 **show ip pim rp** 命令查看 rp 信息是否正确，如果没有 rp 信息，也要检查单播路由；

如果使用检查都尝试仍无法解决 PIM-SM 的问题，那么请使用 debug ip pim/ debug ip pim bsr 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给神州数码技术服务中心。

21.5 DVMRP

21.5.1 DVMRP 介绍

DVMRP（Distance Vector Multicast Routing Protocol）协议即“距离向量组播路由协议”。它是一种密集模式的组播路由协议，采用类似RIP方式的路由交换给每个源建立了一个转发广播树，然后通过动态的剪枝/嫁接给每个源建立起一个截断广播树，也就是到源的最短路径树。通过反向路径检查(RPF)来决定组播包是否应该被转发到下游。

DVMRP 的一些重要特性是：

1. 用于决定反向路径检查信息的路由交换以距离向量为基础（方式与 RIP 相似）
2. 路由交换更新周期性的发生（缺省为 60 秒）
3. TTL 上限＝32 跳（而 RIP 是 16）
4. 路由更新包括掩码，支持 CIDR

相对单播路由来说，组播路由是一种颠倒的路由（也就是，你所感兴趣的是信息包从哪里来而不是到哪里去），因此在DVMRP路由表中的信息是被用于确定是否在正确的接口收到一个输入的组播信息包。否则，为了防止组播循环将放弃该信息包。

把为了确定信息包到达正确的接口所进行的测试称为RPF检查。当有组播数据包到达某个接口，通过查找DVMRP路由表来决定到源网络的反向路径。如果数据包到达的接口是用于向源传送单播信息的接口，则逆向路径检查正确，数据包从所有下游接口转发出去。如果不是，则可能是出现了故障，丢弃该组播包。

因为不是所有的交换机都支持组播，DVMRP支持隧道组播通信，隧道是在被不支持组播路由的交换机隔开的DVMRP交换机之间发送组播数据报的一种方法。它充当两个DVMRP交换机之间的虚拟网络。组播数据包被封装在单播数据包之内，直接发送到下一个支持组播的交换机。DVMRP协议平等对待隧道接口与一般的物理接口。

如果在一个多入口网络上连接了两个或两个以上的交换机，就可能会把一个数据包的多份拷贝发送到该子网上。因此必须指定一个指定的转发者，DVMRP在利用路由交换的机制来达到这一目的，当多入口网络上的两个交换机交换路由信息时，就会互相知道对方到源网络的路由度量，因此到源网路的度量最小的交换机成为该子网上的指定转发者，如果度量一致，则IP地址较低的获胜。

当交换机的某个接口配置了运行DVMRP协议以后，就在该接口上向其他的DVMRP交换机组播探寻（Probe）消息，用于发现邻居且互相探知对方的能力（Capbilities）。如果在邻居超时前一直没有收到该邻居的Probe消息，则认为该邻居丢失。

在DVMRP中，源网络路由选择信息用和RIP相同的基本方式交换。也就是说，路由报告消息定期（缺省为60秒）在DVMRP邻居之间发送。DVMRP路由选择表中的路由信息被用于建立源分布树，也就是决定通过哪一个邻居能够到达发送组播信息的源，到该邻居的接口被称为上游接口。路由报告包含源网络（用掩码）地址和用于路由尺度的跳数项。

为了转发能够正确的完成，每个DVMRP交换机都需要知道那些下游交换机需要通过它从某个特定的源网络接收组播信息。当接收到某个特定的源发来的包后，DVMRP交换机首先从所有的下游接口，也就是在该接口上有其他的对该特定源表示了依赖性的DVMRP交换机，把该组播包广播出去。当接口上收到了某个下游交换机发送的剪枝（Prune）消息后，就把该交换机剪枝。DVMRP交换机使用毒性反转来向通知某个对某个特定源的上游交换机：“我是你的下游”。DVMRP交换机通过把它广播的某个特定源的路由度量加上无限（32）

来回应到该源上游交换机来完成毒性反转。这
意味着度量正确值为1到2*无限（32）-1或1到63，1到31意味着可以到达源网络，32意味着源网络不可达，33到63意味着产生该报告（Report）消息的交换机依赖上游路由器来接收特定源的组播信息。

21.5.2 DVMRP 配置

21.5.2.1 配置任务序列

1、启动 DVMRP（必须）
2、配置和 CISCO 互通（可选）
3、配置 DVMRP 辅助参数（可选）
（1）配置 DVMRP 接口参数
  1）配置 DVMRP report 报文 metric 值
  2）配置 DVMRP 邻居超时时间
（2）配置 DVMRP 全局参数
  1）配置 DVMRP 重传 graft 报文的时间间隔
  2）配置 DVMRP 发送 probe 报文的时间间隔
  3）配置 DVMRP 发送 report 报文的时间间隔
  4）配置 DVMRP 路由超时时间
4、配置 DVMRP 隧道
5、关闭 DVMRP 协议

1. 启动 DVMRP 协议

在 DCRS 系列三层交换机上运行 DVMRP 路由协议的基本配置很简单，只需在相应接口下打开 DVMRP 开关即可。

命令	解释
接口配置模式	
[no] ip dvmrp enable	启动 DVMRP 协议，本命令的 no 操作关闭 DVMRP 协议。（必须）

2. 配置和 CISCO 互通

CISCO 没有实现真正的 DVMRP 协议，其只提供了和 DVMRP 的互通性。由于 CISCO 发送 report 报文，而不发送 probe 报文，因此在和 CISCO 进行互通时需要解决邻居超时问题。配置下面的命令后将根据 report 报文间隔时间来判断邻居是否超时。

命令	解释
接口配置模式	
[no] ip dvmrp cisco-compatible <*A.B.C.D*>	启动和 CISCO 邻居 A.B.C.D 的互通，本命令的 no 操作关闭和 CISCO 邻居的互通。

3. 配置 DVMRP 辅助参数

（1）配置 DVMRP 接口参数

1）配置 DVMRP report 报文 metric 值
2）配置 DVMRP 邻居超时时间

命令	解释
接口配置模式	
ip dvmrp metric <*metric_val*> **no ip dvmrp metric**	配置接口 DVMRP report 报文度量值；本命令的 no 操作恢复为缺省值。
ip dvmrp nbr-timeout <*time_val* > **no ip dvmrp nbr-timeout**	配置接口 DVMRP 邻居超时时间；本命令的 no 操作恢复缺省值。

（2）配置 DVMRP 全局参数

1）配置 DVMRP 发送 graft 报文的时间间隔

2）配置 DVMRP 发送 probe 报文的时间间隔

3）配置 DVMRP 发送 report 报文的时间间隔

命令	解释
全局配置模式	
ip dvmrp graft-interval <*time_val*> **no ip dvmrp graft-interval**	配置周期发送 DVMRP 嫁接消息的时间间隔；本命令的 no 操作恢复缺省值。
ip dvmrp probe-interval <*time_val*> **no ip dvmrp probe -interval**	配置周期发送 DVMRP probe 消息的时间间隔；本命令的 no 操作恢复缺省值。
ip dvmrp report-interval <*time_val*> **no ip dvmrp report-interval**	配置周期发送 DVMRP report 消息的时间间隔；本命令的 no 操作恢复缺省值。

4）配置 DVMRP 路由超时时间

命令	解释
全局配置模式	
ip dvmrp route-timeout <*time_val*> **no ip dvmrp route-timeout**	配置 DVMRP 路由超时时间；本命令的 no 操作恢复为缺省值。

4. 配置 DVMRP 隧道

命令	解释
接口配置模式	
ip dvmrp tunnel <*A.B.C.D*> [metric <*metric_val*>] **no ip dvmrp tunnel <*A.B.C.D*>**	配置到邻居 A.B.C.D 的 DVMRP 隧道；本命令的 no 操作删除到邻居 A.B.C.D 的 DVMRP 隧道。

5. 关闭 DVMRP 协议

命令	解释
接口配置模式	
no ip dvmrp enable	关闭 DVMRP 协议。

21.5.2.2 DVMRP 的配置命令

- **ip dvmrp cisco-compatible**
- **ip dvmrp enable**

- **ip dvmrp graft-interval**
- **ip dvmrp metric**
- **ip dvmrp nbr-timeout**
- **ip dvmrp probe-interval**
- **ip dvmrp report-interval**
- **ip dvmrp route-timeout**
- **ip dvmrp tunnel**
- **show ip dvmrp mroute**
- **show ip dvmrp neighbor**
- **show ip dvmrp route**
- **show ip dvmrp tunnel**
- **debug ip dvmrp detail**
- **debug ip dvmrp pruning**

21.5.2.2.1ip dvmrp cisco-compatible

命令：ip dvmrp cisco-compatible <*A.B.C.D*>
no ip dvmrp cisco-compatible <*A.B.C.D*>
功能：启动和 CISCO 邻居 A.B.C.D 的互通；本命令的 no 操作关闭和 CISCO 邻居的互通。
参数：<*A.B.C.D*>为 CISCO 邻居的 IP 地址。
缺省情况：缺省为不能和 CISCO 邻居保持互通。
命令模式：接口配置模式
使用指南：CISCO 没有实现真正的 DVMRP 协议，其只提供了和 DVMRP 的互通性。由于 CISCO 发送 report 报文，而不发送 probe 报文，因此在和 CISCO 进行互通时需要解决邻居超时问题。配置本命令后将根据 report 报文间隔时间来判断邻居是否超时（如果超过 3 倍 report-interval 时间没有收到 CISCO 邻居的 report 消息，则认为 CISCO 邻居超时）。
举例：设置和 CISCO 邻居 1.1.1.1 保持互通。
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip dvmrp cisco-compatible 1.1.1.1

21.5.2.2.2ip dvmrp enable

命令：ip dvmrp enable
no ip dvmrp enable
功能：配置在接口上启动 DVMRP 协议；本命令的 no 操作在接口上关闭 DVMRP 协议。
参数：无
缺省情况：不启动 DVMRP 协议。
命令模式：接口配置模式
使用指南：
举例：在接口 vlan1 上启动 DVMRP 协议。
Switch (Config)#interface vlan 1
Switch(Config-If-vlan1)#ip dvmrp enable

21.5.2.2.3ip dvmrp graft-interval

命令：ip dvmrp graft-interval <*time_val*>
no ip dvmrp graft-interval
功能：配置周期发送 DVMRP 嫁接消息的时间间隔；本命令的 no 操作恢复缺省值
参数：<*time_val*>为周期发送 DVMRP 嫁接消息的时间间隔，取值范围 5～3600s。
缺省情况：周期发送 DVMRP 嫁接消息的时间间隔缺省为 5s。
命令模式：全局配置模式
使用指南：当某个接口处于剪枝状态时，如果该接口下有新的接收者加入，则需向上游发送嫁接消息；如果不能收到上游发送回来的 graft ACK 消息，则会周期性地向上游发送 graft 消息，直至收到相应的 graft ACK 为止。
举例：配置周期发送 DVMRP 嫁接消息的时间间隔为 10s
Switch (Config)#ip dvmrp graft-interval 10

21.5.2.2.4ip dvmrp metric

命令：ip dvmrp metric <*metric_val*>
no ip dvmrp metric
功能：配置接口 DVMRP report 报文度量值；本命令的 no 操作恢复为缺省值。
参数：< *metric_val* >为度量值，取值范围 1～32。
缺省情况：缺省值为 1。
命令模式：接口配置模式
使用指南：DVMRP report 报文包含的路由信息中包括一组源网络的地址和度量(Metric)的列表，配置了接口 DVMRP report 报文度量值后，将在所有从该接口接收到的路由条目上加上配置的接口度量值作为该路由的新度量值。度量值用于计算毒性反转，即确定上下游关系。如果本交换机上某条路由的度量值大于或等于 32，则说明该路由不可达。如果经计算后判断自己是某条路由的下游，则向上游发送包含该路由的 report 消息，该路由的 metric 在原基础上增加了 32，以表明自己是下游。
举例：配置接口 DVMRP report 报文度量值为 2
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip dvmrp metric 2

21.5.2.2.5ip dvmrp nbr-timeout

命令：ip dvmrp nbr-timeout <*time_val*>
no ip dvmrp nbr-timeout
功能：配置接口 DVMRP 邻居超时时间；本命令的 no 操作恢复缺省值。
参数：<*time_val*>表示邻居超时时间，取值范围为 20～8000s。
缺省情况：邻居超时时间缺省为 35s。
命令模式：接口配置模式
使用指南：DVMRP 确定邻居关系以后，如果在邻居超时时间内没有收到该路由发送过来的 probe 消息，则认为该邻居已经不存在了，从而解除邻居关系。邻居超时时间的配置不能小于发送 probe 消息的周期间隔时间。
举例：配置接口 DVMRP 邻居超时时间为 30s
Switch (Config)#interface vlan 1
Switch(Config-If-vlan1)#ip dvmrp nbr-timeout 30

21.5.2.2.6 ip dvmrp probe-interval

命令：ip dvmrp probe-interval <*time_val*>

no ip dvmrp probe-interval

功能：配置周期发送 DVMRP probe 消息的时间间隔；本命令的 no 操作恢复缺省值

参数：<*time_val*>为周期发送 DVMRP probe 消息的时间间隔，取值范围 5～30s。

缺省情况：周期发送 DVMRP probe 消息的时间间隔缺省为 10s。

命令模式：全局配置模式

使用指南：Probe 消息使得 DVMRP 交换机可以互相定位，确定邻居关系，且可以互相探知对方的能力。DVMRP 交换机通过周期向邻居发送 probe 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的 probe 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。

举例：配置周期发送 DVMRP probe 消息的时间间隔为 20s

Switch (Config)#ip dvmrp probe-interval 20

21.5.2.2.7 ip dvmrp report-interval

命令：ip dvmrp report-interval <*time_val*>

no ip dvmrp report-interval

功能：配置周期发送 DVMRP 路由报告消息的时间间隔；本命令的 no 操作恢复缺省值

参数：<*time_val*>为周期发送 DVMRP 路由报告消息的时间间隔，取值范围 10～2000s。

缺省情况：周期发送 DVMRP 路由报告消息的时间间隔缺省为 60s。

命令模式：全局配置模式

使用指南：DVMRP 路由信息采用和 RIP 协议类似的方式进行交换，即路由报告 report 消息周期性地在 DVMRP 邻居之间发送。如果某条路由在规定的时间内没有从发送该路由的邻居收到更新的 report 消息，则认为该路由已经失效。配置该周期时间不能大于路由的超时时间。

举例：配置周期发送 DVMRP 路由报告消息的时间间隔为 100s

Switch (Config)#ip dvmrp report-interval 100

21.5.2.2.8 ip dvmrp route-timeout

命令：ip dvmrp route-timeout <*time_val*>

no ip dvmrp route-timeout

功能：配置 DVMRP 路由的超时时间；本命令的 no 操作恢复缺省值

参数：<*time_val*>为 DVMRP 路由超时时间，取值范围 20～1400s。

缺省情况：DVMRP 路由超时时间缺省为 140s。

命令模式：全局配置模式

使用指南：如果某条路由在规定的时间内没有从发送该路由的邻居收到更新的 report 消息，则认为该路由已经失效。配置该时间不能小于发送 report 消息的周期间隔时间。

举例：配置 DVMRP 路由的超时时间为 100s

Switch (Config)#ip dvmrp route-timeout 100

21.5.2.2.9ip dvmrp tunnel

命令：ip dvmrp tunnel <*A.B.C.D*> [metric <*metric_val*>]

no ip dvmrp tunnel <*A.B.C.D*>

功能：配置到邻居 A.B.C.D 的 DVMRP 隧道；本命令的 no 操作删除到邻居 A.B.C.D 的 DVMRP 隧道。

参数：<*A.B.C.D*>为远端邻居 IP 地址，**<*metric_val*>**为隧道接口度量值，取值范围 1～32。

缺省情况：缺省为不配置 DVMRP 隧道，**<*metric_val*>**缺省为 1。

命令模式：接口配置模式

使用指南：因为不是所有的交换机都支持组播，DVMRP 支持隧道组播通信，隧道是在被不支持组播路由的交换机隔开的 DVMRP 交换机之间发送组播数据报的一种方法。它充当两个 DVMRP 交换机之间的虚拟网络。组播数据包被封装在单播数据包之内，直接发送到下一个支持组播的交换机。DVMRP 协议平等对待隧道接口与一般的物理接口。

举例：在以太网口 vlan1 上配置到远端邻居 1.1.1.1 的 DVMRP 隧道，metric 为 10。

Switch(Config-If-Vlan1)#ip dvmrp tunnel 1.1.1.1 metric 10

21.5.3　DVMRP 典型案例

如下图，将SWITCHA 和SWITCHB 的以太网接口加入到相应的vlan中，并在各vlan接口上启动DVMRP。

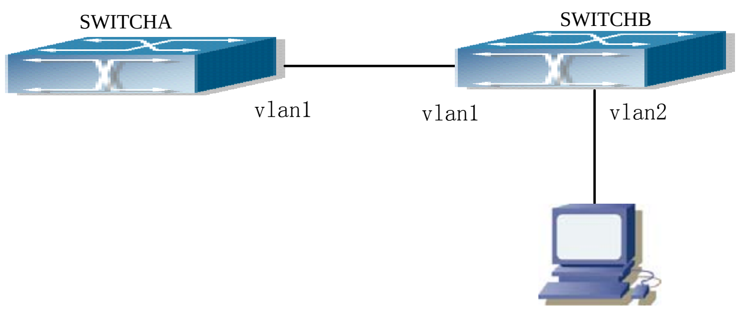


图 21-3 DVMRP 网络拓扑示意图

SWITCHA 和SWITCHB配置步骤如下：

(1) 配置SWITCHA：

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp enable

(2) 配置SWITCHB：

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp enable

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan2)# ip dvmrp enable

21.5.4 DVMRP 排错帮助

1.监测和调试命令
2.DVMRP 排错帮助

21.5.4.1 监测和调试命令

21.5.4.1.1show ip dvmrp mroute

命令：show ip dvmrp mroute
功能：显示 DVMRP 报文转发项。
参数：无。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：本命令用于显示 DVMRP 组播转发项，即系统 FIB 表中用于转发组播报文的转发项。
举例：

```
Switch# show ip dvmrp mroute

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
        Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
        Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

DVMRP Multicast Routing Table, inodes 1 routes 1:

(192.168.1.0, 224.1.1.1), protos: 0x2, flags: 0x0
   Incoming interface : Vlan1, RPF Nbr 0.0.0.0, pref 0, metric 1
  Outgoing interface list:
        (Vlan2), protos: 0x2
  Upstream prune interface list:
  Downstream prune interface list:
```

显示信息	解释
(192.168.1.0, 224.1.1.1)	转发项
Incoming interface	入接口，即 RPF 接口
Outgoing interface list	出接口列表
Upstream prune interface list	上游剪枝接口列表
Downstream prune interface list	下游剪枝接口列表

21.5.4.1.2show ip dvmrp neighbor

命令：show ip dvmrp neighbor [<*ifname*>]
功能：显示 DVMRP 邻居信息。

参数：***<ifname>***为接口名称，即显示指定接
口上的邻居信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：显示以太网口 vlan1 上的邻居信息。
Switch #show ip dvmrp neighbor vlan1
Switch #
  Neighbor-Address Interface Uptime Expires
  192.168.1.22 Vlan1 00:02:22 00:00:28
Switch #

显示信息	解释
Neighbor-Address	邻居地址
Interface	发现该邻居的接口
Uptime	该邻居已存在的时间
Expires	该邻居距离超时还剩的时间

21.5.4.1.3show ip dvmrp route

命令：show ip dvmrp route
功能：显示 DVMRP 路由信息。
参数：无。
缺省情况：不显示。
命令模式：特权用户配置模式
使用指南：本命令用于显示 DVMRP 路由表项；DVMRP 维护单独的单播路由表用于 RPF 检查。
举例：显示 DVMRP 路由信息。
Switch #show ip dvmrp route
Switch #
  Destination/Mask Nexthop Interface Gateway Metric state
  192.168.1.0/24 192.168.1.11 Vlan1 No-Gateway 1 active
Switch #

显示信息	解释
Destination/Mask	目标网段或地址及掩码
Nexthop	下一跳地址
Interface	发现该路由的接口
Gateway	网关地址
Metric	路由度量值
state	路由状态（active、hold 等）

21.5.4.1.4show ip dvmrp tunnel

命令：show ip dvmrp tunnel [<*ifname*>]
功能：显示 DVMRP 隧道信息。
参数：*<ifname>*为接口名称，即显示指定接口上配置的隧道信息。

缺省情况：不显示。
命令模式：特权用户配置模式
举例：显示以太网口 vlan1 上的隧道配置信息。
Switch #show ip dvmrp tunnel vlan1
Name: dvmrp2, Index: 7, State:1195, Parent: 3, Localaddr: 192.168.1.11, Remote: 1.1.1.1
Switch #

显示信息	解释
Name	隧道接口名称（系统自动生成）
Index	隧道接口索引号
State	隧道接口状态
Parent	隧道接口所在父接口的索引号
Localaddr	隧道接口本地地址
Remote	隧道的远端地址

21.5.4.1.5debug ip dvmrp detail

命令：debug ip dvmrp detail
功能：打开显示 DVMRP 详细信息的调试开关；本命令的 no 操作为关闭本调试开关。
参数：无。
缺省情况：关闭。
命令模式：特权用户配置模式
使用指南：如果需要查看 DVMRP 报文（除剪枝和嫁接外）等的详细信息，则可以打开本调试开关。
举例：
Switch#debug ip dvmrp detail
DVMRP detail debug is on
Switch#01:18:09:35: DVMRP: Received probe on vlan1 from 192.168.1.22
01:18:09:35: DVMRP: probe Vers: majorv 3, minorv 255
01:18:09:35: DVMRP: probe flags: PG
01:18:09:35: DVMRP: probe genid: 0x48
01:18:09:35: DVMRP: probe nbrs: 192.168.1.11
01:18:09:40: DVMRP: Send probe on vlan1 to 224.0.0.4, len 16
01:18:09:40: DVMRP: probe Vers: majorv 3, minorv 255
01:18:09:40: DVMRP: probe flags: PG
01:18:09:40: DVMRP: probe genid: 0x24c57
01:18:09:40: DVMRP: probe nbrs: 192.168.1.22
01:18:09:40: DVMRP: Send probe on dvmrp2 to 224.0.0.4, len 12
01:18:09:40: DVMRP: probe Vers: majorv 3, minorv 255
01:18:09:40: DVMRP: probe flags: PG
01:18:09:40: DVMRP: probe genid: 0x24f29

21.5.4.1.6debug ip dvmrp pruning

命令：debug ip dvmrp pruning
no debug ip dvmrp pruning

功能：显示 DVMRP 协议的剪枝、嫁接调试信息；本命令的 no 操作为关闭本调试开关。
参数：无。
缺省情况：不打开调试开关。
命令模式：特权用户配置模式
使用指南：如果需要查看 DVMRP 剪枝、嫁接报文的详细信息，则可以打开本调试开关。
举例：

```
Switch#debug ip dvmrp pruning
DVMRP pruning debug is on
02:22:20:26: DVMRP: Received prune on vlan2 from 105.1.1.2, len 20
02:22:20:26: DVMRP: Prune Vers:   majorv 3, minorv 255
02:22:20:26: DVMRP: Prune source 192.168.1.105, group 224.1.1.1
02:22:20:40: DVMRP: Received graft on vlan1 from 105.1.1.2, len 16
02:22:20:40: DVMRP: Graft Vers:   majorv 3, minorv 255
02:22:20:40: DVMRP: Graft source 192.168.1.105, group 224.1.1.1
02:22:20:40: DVMRP: Send graft-ACK on vlan1 to 105.1.1.2, len 16
02:22:20:40: DVMRP: Graft-Ack Vers:   majorv 3, minorv 255
02:22:20:40: DVMRP: Graft-ACK source 192.168.1.105, group 224.1.1.1
```

21.5.4.2 DVMRP 排错帮助

在配置、使用 DVMRP 协议时，可能会由于物理连接、配置错误等原因导致 DVMRP 协议未能正常运行。因此，用户应注意一下要点：

- ✧ 首先应该保证物理连接的正确无误；
- ✧ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ✧ 请检查接口是否已配置了正确的 IP 地址（使用 ip address 命令）；
- ✧ 然后，在接口上启动 DVMRP 协议（使用 ip dvmrp enable 命令）；
- ✧ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性（DVMRP 使用自己的单播路由表，查看请使用 show ip dvmrp route 命令）；
- ✧ 如果需要和 Cisco 互通，检查是否已经配置 Cisco 互通命令（使用 ip dvmrp cisco-compatible 命令）

如果使用检查都尝试仍无法解决 DVMRP 的问题，那么请使用 debug ip dvmrp detail/prunning 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给神州数码技术服务中心。

21.6 IGMP

21.6.1 IGMP 介绍

IGMP（Internet Group Management Protocol，因特网组管理协议）是TCP/IP协议族中负责IP 组播成员管理的协议。它用来在IP 主机和与其直接相邻的组播交换机之间建立、

维护组播组成员关系。IGMP 不包括组播交换
机之间的组成员关系信息的传播与维护，这部分工作由各组播路由协议完成。所有参与组播的主机必须实现IGMP 协议。

参与IP 组播的主机可以在任意位置、任意时间、成员总数不受限制地加入或退出组播组。组播交换机不需要也不可能保存所有主机的成员关系，它只是通过IGMP 协议了解每个接口连接的网段上是否存在某个组播组的接收者，即组成员。而主机方只需要保存自己加入了哪些组播组。

IGMP 在主机与路由器之间是不对称的：主机需要响应组播交换机的IGMP查询报文，即，以成员资格报告报文响应；交换机周期性发送成员资格查询报文，然后根据收到的响应报文确定某个特定组在自己所在子网上是否有主机加入，并且当收到主机的退出组的报告时，发出特定组的查询（IGMP 版本2），以确定某个特定组是否已无成员存在。

到目前为止，IGMP 有三个版本：IGMP 版本1（由RFC1112 定义）、IGMP版本2（由RFC2236 定义）和IGMP 版本3。目前应用最多的是版本2。

IGMP 版本2 对版本1 所做的改进主要有：

1. 共享网段上组播交换机的选举机制

共享网段即一个网段上有多个组播交换机的情况。在这种情况下，由于此网段下运行IGMP 的交换机都能从主机那里收到成员资格报告消息，因此，只需要一个交换机发送成员资格查询消息，这就需要一个交换机选举机制来确定一个交换机作为查询器。在IGMP 版本1 中，查询器的选择由组播路由协议决定；IGMP 版本2 对此做了改进，规定同一网段上有多个组播交换机时，具有最低IP 地址的组播交换机被选举出来充当查询器。

2. IGMP 版本2 增加了离开组机制

在IGMP 版本1 中，主机悄然离开组播组，不会给任何组播交换机发出任何通知。造成组播交换机只能依靠组播组响应超时来确定组播成员的离开。而在版本2 中，当一个主机决定离开一个组播组时，如果它是对最近一条成员资格查询消息作出响应的主机，那么它就会发送一条离开组的消息。

3. IGMP 版本2 增加了对特定组的查询

在IGMP 版本1 中，组播交换机的一次查询，是针对该网段下的所有组播组。这种查询称为普遍组查询。在IGMP 版本2 中，在普遍组查询之外增加了特定组的查询，这种查询报文的目的IP 地址为该组播组的IP 地址，报文中的组地址域部分也为该组播组的IP 地址。这样就避免了属于其它组播组成员的主机发送响应报文。

4. IGMP 版本2 增加了最大响应时间字段

IGMP 版本2 增加最大响应时间字段，以动态地调整主机对组查询报文的响应时间。

21.6.2 IGMP 配置

21.6.2.1 配置任务序列

1、启动 IGMP（必须）

2、配置 IGMP 辅助参数（可选）

（1）配置 IGMP 组 group 参数

1）配置 IGMP 组过滤条件

2）配置 IGMP 加入组

3）配置 IGMP 加入静态组

（2）配置 IGMP 查询参数

1）配置 IGMP 发送查询报文的时间间隔

2）配置 IGMP 查询的最大反应时间

3）配置 IGMP 查询的超时时间

（3）配置 IGMP 版本

3、 关闭 IGMP 协议

1. 启动 IGMP 协议

在 DCRS 系列三层交换机上没有启动 IGMP 协议的专门命令，在相应接口下启动任何一种组播协议，则 IGMP 自动随之启动。

命令	解释
接口配置模式	
ip dvmrp enable | ip pim dense-mode | ip pim sparse-mode	启动IGMP协议，相应命令的no操作关闭IGMP协议。（必须）

2. 配置 IGMP 辅助参数

（1）配置 IGMP 组 group 参数

1）配置 IGMP 组过滤条件

2）配置 IGMP 加入组

3）配置 IGMP 加入静态组

命令	解释
接口配置模式	
ip igmp access-group {<*acl_num* | *acl_name*>} **no ip igmp access-group**	配置接口对 IGMP 组的过滤条件；本命令的 no 操作取消过滤条件。
ip igmp join-group <*A.B.C.D* > **no ip igmp join-group <*A.B.C.D* >**	配置接口加入某个 IGMP 组；本命令的 no 操作取消加入。
ip igmp static-group <*A.B.C.D* > **no ip igmp static -group <*A.B.C.D* >**	配置接口加入某个 IGMP 静态组；本命令的 no 操作取消加入。

（2）配置 IGMP 查询参数

1）配置 IGMP 发送查询报文的时间间隔

2）配置 IGMP 查询的最大响应时间

3）配置 IGMP 查询的超时时间

命令	解释
接口配置模式	
ip igmp query-interval <*time_val*> **no ip igmp query-interval**	配置周期发送 IGMP 查询消息的时间间隔；本命令的 no 操作恢复缺省值。
ip igmp query-max-response-time <*time_val*> **no ip igmp query-max-response-time**	配置接口对 IGMP 查询的最大反应时间；本命令的 no 操作恢复缺省值。
ip igmrp query-timeout <*time_val*> **no ip igmp query-timeout**	配置接口对 IGMP 查询的超时时间；本命令的 no 操作恢复缺省值。

（3）配置 IGMP 版本

命令	解释
全局配置模式	
ip igmp version <*version*> **no ip igmp version**	配置接口上 IGMP 版本；本命令的 no 操作恢复为缺省值。

3. 关闭 IGMP 协议

命令	解释
接口配置模式	
no ip dvmrp enable | no ip pim dense-mode | no ip pim sparse-mode	关闭 IGMP 协议。

21.6.2.2 IGMP 的配置命令

- **ip igmp access-group**
- **ip igmp join-group**
- **ip igmp query-interval**
- **ip igmp query-max-response-time**
- **ip igmp query-timeout**
- **ip igmp static-group**
- **ip igmp version**
- **show ip igmp groups**
- **show ip igmp interface**
- **debug ip igmp event**
- **debug ip igmp packet**

21.6.2.2.1ip igmp access-group

命令：**ip igmp access-group {<*acl_num* | *acl_name*>}**
no ip igmp access-group
功能：配置接口对 IGMP 组的过滤条件；本命令的 no 操作取消过滤条件。
参数：**{<*acl_num* | *acl_name*>}**为 access list 的序号或名称，其中 ***acl_num*** 的取值范围为 1～99。
缺省情况：缺省为无过滤条件。
命令模式：接口配置模式
使用指南：可以配置接口对组进行过滤，允许或拒绝某些组的加入。
举例：配置接口 vlan1 接受组 224.1.1.1，拒绝组 224.1.1.2。

```
Switch (Config)#access-list 1 permit 224.1.1.1 0.0.0.0
Switch (Config)#access-list 1 deny 224.1.1.2 0.0.0.0
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip igmp access-group 1
```

21.6.2.2.2ip igmp join-group

命令：ip igmp join-group <*A.B.C.D* >

no ip igmp join-group <*A.B.C.D* >

功能：配置接口加入某个 IGMP 组；本命令的 no 操作取消加入。

参数：<*A.B.C.D* >为组地址

缺省情况：不加入组。

命令模式：接口配置模式

使用指南：当把交换机当做 HOST 时，本命令配置 HOST 加入某个组；即如果配置本接口加入组 224.1.1.1，则当交换机收到其它交换机发送过来的 IGMP 组查询时，将发送 IGMP 成员报告，报告中包含组 224.1.1.1。请注意本命令和 **ip igmp static-group** 命令的区别。

举例：在接口 vlan1 上配置加入组 224.1.1.1。

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1

21.6.2.2.3ip igmp query-interval

命令：ip igmp query-interval <*time_val*>

no ip igmp query-interval

功能：配置周期发送 IGMP 查询消息的时间间隔；本命令的 no 操作恢复缺省值。

参数：<*time_val*>为周期发送 IGMP 查询消息的时间间隔，取值范围 1～65535s。

缺省情况：周期发送 IGMP 查询消息的时间间隔缺省为 125s。

命令模式：接口配置模式

使用指南：当某个接口启动某种组播协议后，会周期性地在该接口上发送 IGMP 查询消息，本命令用于配置该查询周期时间。

举例：配置周期发送 IGMP 查询消息的时间间隔为 10s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-interval 10

21.6.2.2.4ip igmp query-max-response-time

命令：ip igmp query-max-response-time <*time_val*>

no ip igmp query- max-response-time

功能：配置接口对 IGMP 查询的最大响应时间；本命令的 no 操作恢复缺省值。

参数：<*time_val*>为接口对 IGMP 查询的最大响应时间，取值范围 1～25s。

缺省情况：缺省为 10s。

命令模式：接口配置模式

使用指南：从交换机接收到一条查询消息后，主机会为其所属的每个组播组都设置一个计时器，计时器的值在0～最大响应时间中随机选定，当其中任何一个计时器的值减为0 时，主机就会发送该组播组的成员报告消息。合理设置最大响应时间，可以使主机快速响应查询信息，路由器也就能快速地掌握组播组成员的存在状况。

举例：配置对 IGMP 查询消息进行响应的最大时间为 20s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query- max-response-time 20

21.6.2.2.5ip igmp query-timeout

命令：ip igmp query-timeout <*time_val*>

no ip igmp query-timeout

功能：配置接口对 IGMP 查询的超时时间；本命令的 no 操作恢复缺省值。

参数：<*time_val*>为 IGMP 查询的超时时间，取值范围 60～300s。

缺省情况：缺省为 265s。

命令模式：接口配置模式

使用指南：在共享网络上，当存在多个运行IGMP的交换机时，将选举出其中一台交换机作为该共享网络上的查询器，其它交换机则起一个定时器监控查询器的状态；当经过查询超时时间仍未收到查询器发送的查询报文，则重新选举另一交换机成为新的查询器。

举例：配置接口对 IGMP 查询的超时时间 100s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-timeout 100

21.6.2.2.6ip igmp static-group

命令：ip igmp static-group <*A.B.C.D* >

no ip igmp static -group <*A.B.C.D* >

功能：配置接口加入某个 IGMP 静态组；本命令的 no 操作取消加入。

参数：<*A.B.C.D* >为组地址

缺省情况：不加入静态组。

命令模式：接口配置模式

使用指南：当配置某接口加入某个静态组后，则无论该接口下是否有实际的接收者，都将接收关于该静态组的组播包；即如果配置本接口加入静态组 224.1.1.1，则本接口一直会接收关于组 224.1.1.1 的组播报文，而不管接口下是否有接收者。请注意本命令和 **ip igmp join-group** 命令的区别。

举例：在接口 vlan1 上配置加入静态组 224.1.1.1。

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1

21.6.2.2.7ip igmp version

命令：ip igmp version <*version*>

no ip igmp version

功能：配置接口上 IGMP 版本；本命令的 no 操作恢复为缺省值。

参数：<*version*>为配置的 IGMP 版本，目前支持版本 1 和版本 2。

缺省情况：缺省为版本 2。

命令模式：接口配置模式

使用指南：该命令主要用于提供不同版本之间的前向兼容性；需注意的是版本 1 和版本 2 之间是不能互通的，因此在同网络内必须配置成相同版本的 IGMP。

举例：配置接口运行的 IGMP 为版本 1

Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip igmp version 1

21.6.3 IGMP 典型案例

如下图，将SWITCHA 和SWITCHB 的以太网端口加入相应的vlan，并在各vlan接口上启动PIM-DM。

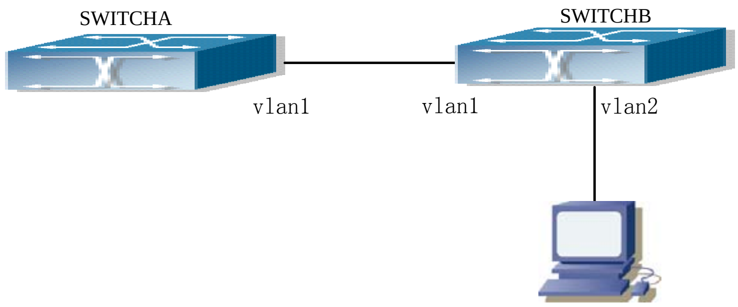


图 21-4 IGMP 网络拓扑示意图

SWITCHA 和SWITCHB配置步骤如下：
(1) 配置SWITCHA：
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip pim dense-mode
(2) 配置SWITCHB：
Switch(Config)#interface vlan1
Switch(Config-If-Vlan1)#ip pim dense-mode
Switch(Config-If-Vlan1)#exit
Switch(Config)#interface vlan2
Switch(Config-If-Vlan2)#ip pim dense-mode
Switch(Config-If-Vlan2)#ip igmp version 1
Switch(Config-If-Vlan2)#ip igmp query-timeout 150

21.6.4 IGMP 排错帮助

1.监测和调试命令
2.IGMP 排错帮助

21.6.4.1 监测和调试命令

21.6.4.1.1show ip igmp groups

命令：**show ip igmp groups [{<*ifname* | *group_addr*>}]**

功能：显示 IGMP 组信息。
参数：***<ifname>***为接口名，即查看指定接口上的组信息；***<group_addr>***为组地址，即查看指定组信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：
Switch#show ip igmp groups
IGMP Connect Group Membership (1 group(s) joined)
Group Address   Interface   Uptime   Expires   Last Reporter
239.255.255.250   Vlan123   02:57:30   00:03:36   123.1.1.2
Switch#

显示信息	解释
Group Address	组播组 IP 地址
Interface	组播组所属的接口
Uptime	组播组已经存在的时间
Expires	组播组离超时所剩时间
Last Reporter	最后报告该组播组的主机

21.6.4.1.2 show ip igmp interface

命令：**show ip igmp interface [<*ifname*>]**
功能：显示接口上相关 IGMP 信息。
参数：***<ifname>***为接口名称，即显示指定接口上的 IGMP 信息。
缺省情况：不显示。
命令模式：特权用户配置模式
举例：显示以太网口 vlan1 上的 IGMP 信息。
Switch # show ip igmp interface vlan1
Vlan1 is up, line protocol is up
  Internet address is 192.168.1.11, subnet mask is 255.255.255.0
  IGMP is enabled, I am querier
  IGMP current version is V2
  IGMP query interval is 125s
  IGMP querier timeout is 265s
  IGMP max query response time is 10s
  Inbound IGMP access group is not set
  Multicast routing is enable on interface
  Multicast TTL threshold is 1
  Multicast designed router (DR) is 192.168.1.22
  Muticast groups joined by this system: 0

21.6.4.1.3 debug ip igmp event

命令：**debug ip igmp event**
功能：打开显示 IGMP 事件的调试开关；本命令的 no 操作为关闭本调试开关。

参数：无。
缺省情况：关闭。
命令模式：特权用户配置模式
使用指南：如果需要查看 IGMP 事件信息，则可以打开本调试开关。
举例：
Switch# debug ip igmp event
igmp event debug is on
Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

21.6.4.1.4debug ip igmp packet

命令：**debug ip igmp packet**
功能：打开显示 IGMP 报文信息的调试开关；本命令的 no 操作为关闭本调试开关。
参数：无。
缺省情况：关闭。
命令模式：特权用户配置模式
使用指南：如果需要查看 IGMP 报文信息，则可以打开本调试开关。
举例：
Switch# debug ip igmp packet
igmp packet debug is on
Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0
02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0
.0.0
02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0
02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0
.0.0

21.6.4.2 IGMP 排错帮助

在配置、使用 IGMP 协议时，可能会由于物理连接、配置错误等原因导致 IGMP 协议未能正常运行。因此，用户应注意以下要点：

- 首先应该保证物理连接的正确无误；
- 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- 然后，确保在接口上启动一种组播协议；
- 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性；

如果使用检查都尝试仍无法解决 IGMP 的问题，那么请使用 debug ip igmp event/packet 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给神州数码技术服务中心。

第22章HS RP 配置

22.1 HSRP 简介

终端可以使用多种方法决定它们到特定 IP 地址的第一跳。常用的方法有两种：一种是动态学习，如代理 ARP，路由协议（RIP 和 OSPF）以及 IRDP（ICMP Router Discovery Protocol）；另一种是静态配置。在每一个终端都运行动态路由协议是不现实的，大多客户端操作系统平台都不支持动态路由协议，即使支持也受到管理开销、收敛度、安全性等许多问题的限制。因此普遍采用对终端 IP 设备静态路由配置，一般是给终端设备指定一个或者多个默认网关(Default Gateway)。静态路由的方法简化了网络管理的复杂度和减轻了终端设备的通信开销，但是它仍然有一个缺点：如果作为默认网关的交换机损坏，所有使用该网关为下一跳主机的通信必然要中断。即便配置了多个默认网关，如不重新启动终端设备，也不能切换到新的网关。HSRP 就是为了避免静态指定网关的缺陷。

HSRP 在以太网上的应用是两台或多台交换机之间实现备份，这些交换机称作一个备份组。它们协同工作，在局域网上的主机看来像一台虚拟交换机。在一个备份组内，只有一台交换机承担报文转发任务，这台交换机称作活动交换机，同时存在一个主备用交换机和任意个数的备用交换机。当活动交换机出现故障后，备份交换机能够自动接管它的报文转发工作，从而提供不中断的网络服务。该协议通常用来防止第一跳交换机的故障而引起的通信中断，因为在通常情况下，源主机不能动态地学到第一跳的交换机的 IP 地址。HSRP 的优点就是它具有更高的实用性，并且它无须在每个终端都配置动态路由或寻找路由的协议。当一台交换机不可用时，由配置的其他交换机来接管其功能，保证通信的不中断。HSRP 允许两台或多台交换机使用一台虚拟交换机的 MAC 和 IP 地址。虚拟交换机并不实际存在，它只表示一组配置的相互之间备份的交换机。

活动交换机是指处于活动状态的运行 HSRP 的交换机，是物理实体，负责数据报文转发的工作。虚拟交换机是 HSRP 协议创建的，是逻辑概念。一组 HSRP 交换机协同工作，共同构成一台虚拟交换机。该虚拟交换机对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑交换机。HSRP 协议使用选择策略从交换机组中选出一台作为主控，负责 ARP 和转发 IP 数据包，另外一个交换机作为备份的角色处于待命状态。当由于某种原因主控交换机发生故障时，主备份交换机能在几秒钟的时延后升级为活动交换机。由于切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对终端使用者系统是透明的。

22.2 HSRP 配置

22.2.1 配置任务序列

1. 启动/关闭 HSRP（必须）
2. 配置 HSRP 认证（可选）
3. 配置 HSRP 辅助参数（可选）

（1）配置 HSRP 抢占模式
（2）配置 HSRP 优先级
（3）配置 HSRP 定时器时间间隔

1.启动/关闭 HSRP

命令	解释
VLAN 接口配置模式	
[no] standby [<*group*>] ip [<*A.B.C.D*>]	启动/关闭 HSRP。

2.配置 HSRP 认证

命令	解释
全局配置模式	
standby [*group*] authentication <*string*> **no standby [*group*] authentication**	配置 HSRP 认证；本命令的 no 操作为恢复 HSRP 缺省认证方式。

3.配置 HSRP 辅助参数

（1）配置 HSRP 抢占模式

命令	解释
VLAN 接口配置模式	
[no] standby [*group*] preempt	配置 HSRP 为抢占模式；本命令的 no 操作为取消抢占模式。

（2）配置 HSRP 优先级

命令	解释
VLAN 接口配置模式	
standby [*group*] priority <*value*> **no standby [*group*] priority**	配置 HSRP 优先级；本命令的 no 操作为恢复优先级为缺省值。

（3）配置 HSRP 定时器时间间隔

命令	解释
VLAN 接口配置模式	
standby [*group*] timers <*hello_time*> <*hold_time*> **no standby [*group*] timers**	配置 HSRP 定时器时间值；本命令的 no 操作为恢复缺省值。

22.2.2 HSRP 配置命令

22.2.2.1 standby authentication

命令：**standby [<*group*>] authentication <*string*>**
no standby [<*group*>] authentication

功能：配置 HSRP 认证；本命令的 no 操作为恢复 HSRP 缺省认证方式。

参数：***<group>***为组序号，取值范围为 0～255；***<string>***为认证字符串，长度为 1～8 个字符。
缺省情况：缺省认证字符串为“DCN”；***<group>***如不指定，缺省为 0。
命令模式：VLAN 接口配置模式
使用指南：该命令用于避免 HSRP 备份组受到非授权成员的干扰，同一备份组内的所有交换机应设为相同的字符串。
举例：配置组 10 的认证授权字符串为“public”。
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#standby 10 authentication public

22.2.2.2 standby ip

命令：**standby [<*group*>] ip [<*A.B.C.D*>]**
no standby [<*group*>] ip [<*A.B.C.D*>]
功能：启动/关闭 HSRP。
参数：***<group>***为组序号，取值范围为 0～255；***<A.B.C.D>***为虚拟 IP 地址。
缺省情况：缺省为不配置；***<group>***如不指定，缺省为 0；***<A.B.C.D>***如不指定，缺省为 0.0.0.0。
命令模式：VLAN 接口配置模式
使用指南：启动 HSRP，如果虚拟 IP 地址不指定，交换机不会参与备份，直到从备份组中的活动交换机获得虚拟 IP 地址。虚拟 IP 应该是接口所在的网段内的地址。一旦退出 HSRP 备份组，则交换机在该组上设置的其他属性都不再起作用。
举例：配置组 10 的虚拟 ip 地址为 10.1.1.1
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#standby 10 ip 10.1.1.1

22.2.2.3 standby preempt

命令：**standby [<*group*>] preempt**
no standby [<*group*>] preempt
功能：配置 HSRP 为抢占模式；本命令的 no 操作为取消抢占模式。
参数：***<group>***为组序号，取值范围为 0～255。
命令模式：VLAN 接口配置模式
缺省情况：缺省为不抢占；***<group>***缺省为 0。
使用指南：如果需要高优先级的交换机能主动抢占成为活动交换机，则要设置抢占模式。
举例：配置本交换机 VLAN1 对组 10 为抢占模式
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#standby 10 preempt

22.2.2.4 standby priority

命令：**standby [<*group*>] priority <*value*>**
no standby [<*group*>] priority
功能：配置 HSRP 优先级；本命令的 no 操作恢复优先级为缺省值。

参数：**<*group*>**为组序号，取值范围为 0～255；**<*value*>**为优先级，取值范围为 0～255。
缺省情况：**<*group*>**缺省为 0；优先级缺省值为 100。
命令模式：VLAN 接口配置模式
使用指南：优先级将决定一台交换机在 HSRP 备份组中的状态，优先级最高的交换机将成为活动交换机，其他低优先级的交换机将成为备份交换机。
举例：配置本交换机 VLAN1 对组 10 的优先级为 120
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#standby 10 priority 120

22.2.2.5 standby timers

命令：**standby [<*group*>] timers <*hello_time*> <*hold_time*>**
no standby [<*group*>] timers
功能：配置 HSRP 定时器时间值；本命令的 no 操作为恢复缺省值。
参数：**<*group*>**为组序号，取值范围为 0～255；**<*hello_time*>**为 HSRP 定时发送 Hello 报文的时间间隔，取值范围为 1～254；**<*hold_time*>**为 HSRP 认为成员无效的超时时间间隔，取值范围为 2～255。
缺省情况：**<*group*>**缺省为 0；**<*hold_time*>**缺省值为 3s；**<*hello_time*>**缺省值为 10s。
命令模式：VLAN 接口配置模式
使用指南：HSRP 备份组成员每隔 hello_time 发 Hello 报文通知其他成员，如果经过 hold_time 没有收到某成员的 Hello 报文则认为它已经无效；同一备份组的各成员要设置相同的 hello_time 和 hold_time，且 hold_time 必须大于 hello_time。
举例：设置组 10 的 hello_time 为 10，hold_time 为 30
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#standby 10 timers 10 30

22.2.3 HSRP 典型案例

如下图，SWITCHA 和 SWITCHB 在同一组内互为备份交换机，配置 SWITCHB 为活动交换机。

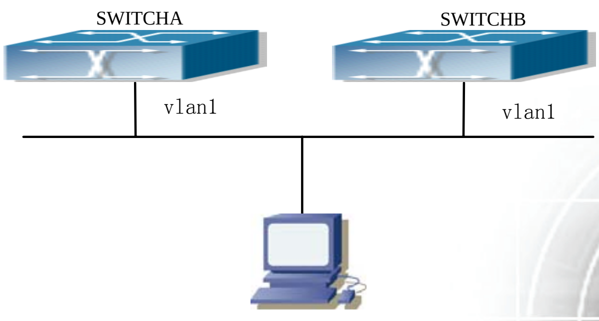


图 22-1 HSRP 网络拓扑示意图

SWITCHA 的配置：
SwitchA(config)#interface vlan 1
SwitchA(Config-If-Vlan1)#ip address 10.1.1.5 255.255.255.0
SwitchA(Config-If-Vlan1)#standby 10 ip 10.1.1.1
SwitchA(Config-If-Vlan1)#standby 10 authentication DCN
SwitchA(Config-If-Vlan1)#standby 10 preempt
SwitchA(Config-If-Vlan1)#standby 10 priority 10
SWITCHB 的配置：
SwitchB(config)#interface vlan 1
SwitchB(Config-If-Vlan1)#ip address 10.1.1.3 255.255.255.0
SwitchB(Config-If-Vlan1)#standby 10 ip 10.1.1.1
SwitchB(Config-If-Vlan1)#standby 10 authentication DCN
SwitchB(Config-If-Vlan1)#standby 10 preempt
SwitchB(Config-If-Vlan1)#standby 10 priority 20

22.2.4 HSRP 排错帮助

22.2.4.1 监测和调试的命令

22.2.4.1.1show standby

命令：show standby [<***vlan information***>][**<*ifname*>**]
功能：显示 HSRP 备份组的状态和配置信息。
命令模式：特权用户配置模式
举例：
Switch# show standby

****
Vlan12 - Group1
Local state is   ACTIVE (interface   up) ,priority 100(default)
Hello time 3 sec, hold time 10 sec(Default)
Authentication is DCN(Default)
Preemption disabled
Virtual IP address is 12.1.1.3
Active router is local,Priority 100 (default 100)
Standby router is unknown!

****
Switch#

显示信息	解释
VLAN12	接口名称；

Group	组序号；
Local state	本接口所处状态；
priority	优先级；
Hello time	发送 hello 报文的周期时间；
hold time	超时时间；
Authentication	认证字符串；
Preemption	抢占模式；
Virtual IP address	虚拟 IP 地址
Active router	本组活动路由器（交换机）；
Priority	优先级；
Standby router	本组备份路由器（交换机）；

22.2.4.1.2 debug standby

命令：debug standby [**error | event | packet** [**hello | coup | resign**]]
no debug standby [**error | event | packet** [**hello | coup | resign**]]
功能：显示 HSRP 备份组的状态变化和收发报文的情况；本命令的 no 操作是关闭 DEBUG 显示。
缺省情况：缺省调试开关是关闭的。
命令模式：特权用户配置模式
举例：

```
Switch#debug standby
Event:Hello timer expiry happen on interface Vlan12 group 1
Hello pkt is sent,on interface Vlan12 group 1 from 12.1.1.1
Event:Hello timer expiry happen on interface Vlan12 group 1
Hello pkt is sent,on interface Vlan12 group 1 from 12.1.1.1
Event:Hello timer expiry happen on interface Vlan12 group 1
Hello pkt is sent,on interface Vlan12 group 1 from 12.1.1.1
Event:Hello timer expiry happen on interface Vlan12 group 1
Hello pkt is sent,on interface Vlan12 group 1 from 12.1.1.1
nEvent:Hello timer expiry happen on interface Vlan12 group 1
Hello pkt is sent,on interface Vlan12 group 1 from 12.1.1.1
```

22.2.4.2 HSRP 排错帮助

在配置、使用 HSRP 协议时，可能会由于物理连接、配置错误等原因导致 HSRP 协议未能正常运行。因此，用户应注意以下要点：

- ✧ 首先应该保证物理连接的正确无误；
- ✧ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ✧ 然后，确保在接口上已启动了 HSRP 协议；
- ✧ 检查同一备份组内的不同交换机认证是否相同；
- ✧ 检查同一备份组内的不同交换机配置的 timer 时间是否相同；

✧ 检查虚拟 IP 地址是否和接口真实 IP 地址
在同一网段内；

如果使用检查都尝试仍无法解决 HSRP 的问题，那么请使用 debug standby 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给神州数码技术服务中。